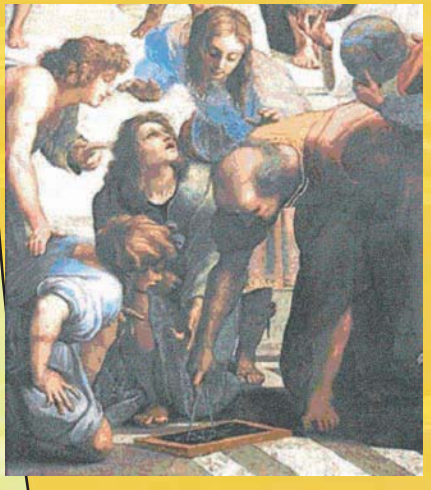
Chapitre 9

# ARITHMETIQUE

**I** . Divisibilité dans $\mathbb{Z}$
**II** . Division euclidienne
**III** . Congruences
**IV** . PGCD et PPCM de deux entiers
**V** . Théorème de Bézout
**VI** . Lemme de Gauss
**VII** . Application : résolution dans $\mathbb{Z} \times \mathbb{Z}$ d'équations du type $ax+by = c$ où $a$, $b$ et $c$ sont des entiers relatifs



**Euclide dans l'école d'Athènes de Raphaél**
**(Musée du Vatican)**

# I. Divisibilité dans $\mathbb{Z}$

## Activités préliminaires

### Activité 1 :

Montrer que, pour tout $n \in \mathbb{N}$, $3^{n+5} - 3^n$ est un multiple de 11.

### Activité 2 :

1) Vérifier que 111 est un multiple de 37
2) En déduire que tout nombre de trois chiffres identiques en base décimale est un multiple de 37

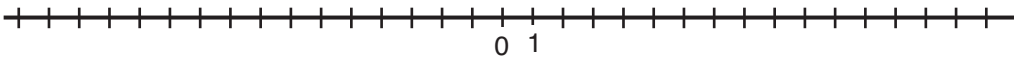
### Activité 3 :

On choisit un entier s'écrivant avec quatre chiffres, par exemple 7892 puis on l'écrit «à l'envers» : 2987.
On fait la somme des deux nombres obtenus. Obtient-on un multiple de 11 ?
Recommencer avec d'autres nombres de quatre chiffres. Expliquer le phénomène observé.

## Activités de découverte

### Activité 1 :

Reproduire la droite réelle ci-dessous




1) Repérer en vert sur cette droite l'ensemble $E$ des entiers relatifs de la forme 4k où $k \in \mathbb{Z}$.
2) Repérer en rouge sur cette droite l'ensemble $F$ des entiers relatifs de la forme $(-4)k$ où $k \in \mathbb{Z}$. Que constate-t-on ?

➢ Tout entier relatif de la forme $4k$ où $k \in \mathbb{Z}$, s'appelle **multiple** de 4 dans $\mathbb{Z}$ .

➢ L'ensemble de multiples de $a$ est identique à l'ensemble de multiples de $(-a)$.

3) Choisir deux multiples de 4 et en faire la somme. Obtient-on encore un multiple de 4 ? Enoncer une propriété générale et la démontrer.
4) On considère deux multiples consécutifs de 4. Si le plus petit s'écrit $4k$ où $k$ est un entier, comment s'écrit le suivant ? Comment s'écrivent les nombres qui sont compris entre ces deux multiples consécutifs ?

### Activité 2 :

1) Soit $a$ un entier relatif non nul, citer quatre diviseurs distincts de $a$ .
2) Soit $a$ un entier relatif non nul, montrer que si un entier $b$ divise $a$ alors $-|a| \leq b \leq |a|$ .
En déduire que tout entier non nul admet un nombre fini de diviseurs.

### Activité 3 :

$a,b,c$ désignent des entiers relatifs non nuls et différents de 1. Démontrer les propriétés suivantes :

1) Si $a$ divise $b$ et $b$ divise $a$ alors $a = b$ ou $a = -b$.
2) Si $a$ divise $b$ et $b$ divise $c$ alors $a$ divise $c$ .
3) Si $a$ divise $b$ et $c$ , aalors, pour tout entiers relatifs $n$ et $m$, $a$ divise $nb + mc$

## A retenir

### Définitions

Soient $a$ et $b$ deux entiers relatifs.
On dit que $a$ **est un multiple de** $b$ s'il existe un entier relatif $k$ tel que $a = kb$.
Si $b \neq 0$, dire que $b$ divise $a$ signifie qu'il existe un entier relatif $k$ tel que $a = k\,b$, c'est à dire, que $a$ est un multiple de $b$.

### Remarques

- Les multiples d'un entier $a$ sont les nombres : $0, a, 2a, \ldots, k\,a$ …et $0, -a\ -2a, \ldots, -k\,a, \ldots$
- Tout entier relatif $a$ non nul et différent de 1 admet au moins quatre diviseurs entiers relatifs : $1,\ -1,\ a\ ,\ -a$.
- Si $a \neq 0$, tout diviseur $b$ de $a$ vérifie $-|a| \leq b \leq |a|$ .
- Tout entier relatif non nul $a$ divise 0, mais 0 ne divise acun entier relatif.

### Propriétés

$a,b$ et $c$ désignent des entiers relatifs non nuls.

- Si $a$ divise $b$ alors $-a$ divise $b$.
- Si $a$ divise $b$ et $b$ divise $a$ alors $a = b$ ou $a = -b$ .
- Si $a$ divise $b$ et $b$ divise $c$ alors $a$ divise $c$ .
- Si $a$ divise $b$, alors pour tout entier relatif non nul $k$ , $ka$ divise $kb$.
- Si $a$ divise $b$ et $c$, alors pour tous entiers relatifs $n$ et $m$, $a$ divise $nb + mc$ .

## Applications

1 1) Déterminer la liste des diviseurs positifs de chacun des entiers : 72 ; 75 ; 83 ; 120 ; 200.
2) Déterminer la liste des diviseurs de chacun des entiers relatifs : 50 ; -56 ; -8 ; 63.

2 Démontrer que la somme de trois entiers relatifs consécutifs est divisible par 3.

3 Comment choisir l'entier relatif $n$ pour que $n$ divise $n + 8$ ?

4 $n$ étant un entier relatif. Démontrer que $n(n^2-1)$ est un multiple de 2 et un multiple de 3.

5 Déterminer les entiers $n$ pour que les rationnels suivants soient des entiers relatifs :

a) $\dfrac{n+2}{n-4}$ ; b) $\dfrac{2n+8}{n-2}$ ; c) $\dfrac{7n-1}{n+3}$ ; d) $\dfrac{-6n+3}{n+5}$

## II. Division euclidienne

### Activités préliminaires

Activité 1 :

Dans chaque cas, écrire la division euclidienne de $a$ par $b$ :

a) $a = 2007$ et $b = 35$ ; b) $a = 5000$ et $b = 17$ ; c) $a = 18$ et $b = 50$ .

Activité 2:

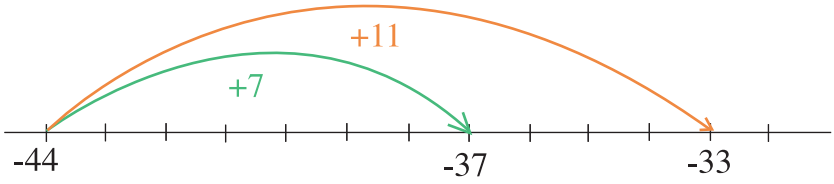
$A$ et $B$ sont deux entiers naturels vérifiant $A = 13B + 50$ .

Ecrire la division euclidienne : a) de $A$ par 13 ; b) de $3A + 20$ par 13.

### Activités de découverte

Activité 1 :

1) Encadrer -37 par deux multiples consécutifs de 11.




2) Vérifier alors que : $-37 = -44 + 7 = 11 \times (-4) + 7$.

➢ La dernière égalité traduit ce qu'on appelle **la division euclidienne de** - 37 par 11.

**Le reste** de cette division est l'entier positif 7.

3) A partir de l'égalité : $-356 = 17 \times (-20) - 16$, compléter l'égalité : $-356 = 17 \times (\ldots) + 1$.

4) Quel reste obtient-on en divisant - 37 par - 4 ?

➢ De façon générale, si $a$ et $b$ sont deux entiers relatifs tel que $b$ est non nul, effectuer **la division euclidienne de** $a$ **par** $b$, c'est trouver le couple $(q\ ;\ r)$ d'entiers relatifs tels que :

$$a = bq + r \quad \text{et} \quad 0 \leq r < |b|$$

5) Ecrire la division euclidienne de 118 par 23, puis celle de - 118 par 23, de 118 par - 23, de -118 par -23.

Activité 2 :

1) $a$ et $b$ sont deux entiers relatifs tels que $b$ est non nul. En effectuant la division euclidienne de $a$ par $b$, quelles sont les valeurs possibles du reste ?

2) Expliquer pourquoi tout entier $a$ peut s'écrire sous la forme $2k$ ou $2k + 1$ avec $k \in \mathbb{Z}$ .

3) Démontrer que le nombre $A = n(n^2 + 5)$ où $n$ est entier relatif, est divisible par 3.

## A retenir

**Théorème (admis)**

Soit $a$ un entier relatif et $b$ un entier relatif non nul. Il existe un unique couple $(q,r)$ d'entiers relatifs vérifiant à la fois : $a = bq + r$ et $0 \leq r < |b|$ .

**Définitions**

Soit $a$ un entier relatif et $b$ un entier relatif non nul.

Effectuer **la division euclidienne de *a* par *b***, c'est trouver le couple d'entiers relatifs $(q,r)$ tels que : $a = bq+r$ et $0 \leq r < |b|$ .

$q$ est **le quotient**, $r$ est **le reste**, $a$ s'appelle le **dividende** et $b$ le **diviseur**.

**Remarques**

Si $a = bq+r$ et $0 \leq r < |b|$ .

- $b$ divise $a$ si et seulement si le reste $r$ est nul.
- Le reste ne peut prendre que l'une des valeurs parmi 0 ; 1 ; 2 ;.... ; $|b|$ -1.
- $b$ étant fixé, les entiers relatifs peuvent être classés selon leur reste dans la division euclidienne par $b$ .

### Applications

1 Déterminer le quotient $q$ et le reste $r$ de la division euclidienne de $a$ par $b$ .

a) $a = 117; b = 28$ b) $a = -317; b = 21$ ; c) $a = -671 ; b = -6$

Sachant que 287025 = 635 x 452 + 5.

2 Déterminer le quotient et le reste de la division euclidienne de :

a) - 287 025 par 635 b) - 287 025 par 452

3 Soit $m$ et $n$ deux entiers naturels.

Les restes de la division euclidienne de $m$ et $n$ par 11 sont respectivement 2 et 7.

Déterminer le reste de la division euclidienne des nombres $m+n$ et $m-n$ par 11. En déduire celui de $m^2 - n^2$ .

4 Déterminer les entiers naturels $a,b$ et $c$ tels que : $\frac{59}{3^2} = a + \frac{b}{3} + \frac{c}{3^2}$.

## III. Congruences

### Activités de découverte

Activité 1 :

Le 1er janvier 2010 est vendredi, quel jour de la semaine sera le 20 mars 2015 ?

Activité 2 :

On a écrit les entiers par rangées de 2, de 3, de 4, … dans différents tableaux.

Quelle propriété commune ont tous les entiers d'une même colonne d'un tableau ?

| | |
|---|---|
| 0 | 1 |
| 2 | 3 |
| 4 | 5 |
| 6 | 7 |
| 8 | 9 |
| 10 | 11 |
| 12 | 13 |

| | | |
|---|---|---|
| 0 | 1 | 2 |
| 3 | 4 | 5 |
| 6 | 7 | 8 |
| 9 | 10 | 11 |
| 12 | 13 | 14 |
| 15 | 16 | 17 |
| 18 | 19 | 20 |

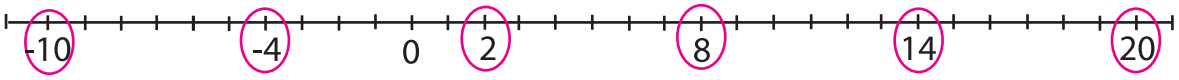
| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 |

| | | | | |
|---|---|---|---|---|
| 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 | 29 |
| 30 | 31 | 32 | 33 | 34 |

## Activité 3 :

$a$ et $a'$ étant deux entiers relatifs quelconques, on se demande à quelle condition $a$ et $a'$ ont le même reste lorsqu'on les divise par un entier naturel non nul $n$ .

1) Le dessin ci-dessous indique des nombres qui « divisés par 6 donnent un reste égal à 2 ».




Que peut-on dire de la différence entre deux d'entre eux ?

2) Sachant que $a = n\,q + r$ et $a' = n\,q' + r'$ avec $0 \le r < n$ *et* $0 \le r' < n$,
vérifier que lorsque $a$ et $a'$ ont le même reste dans la division euclidienne par $n$, $a - a'$ est un multiple de $n$.

Réciproquement, supposer que $a - a' = n\,k$ et que $a = n\,q + r$. Prouver que $r$ est aussi le reste de la division de $a'$ par $n$ .

➢ On dit que $a$ et $a'$ sont **congrus** modulo $n$, et on note $a \equiv a'\left[n\right]$
(on lit a congru à $a'$ modulo $n$)

Vérifier les congruences suivantes :

- $a \equiv a\left[n\right]$ pour tout entier naturel non nul.
- $a \equiv r\left[n\right]$ lorsque $r$ est le reste da la division euclidienne de $a$ par $n$.

- $14 \equiv 2\left[6\right]$ ; $-2 \equiv 5\left[7\right]$; $27 \equiv -3\left[10\right]$

Activité 4 :

$a$, $b$, $c$ et $d$ sont des entiers relatifs, $n$ un entier naturel non nul. En utilisant la définition d'une congruence, prouver les résultats suivants :

1) Si $a \equiv b\,[n]$ alors $b \equiv a\,[n]$

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

3) Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$ alors

- $a + c \equiv b + d\,[n]$ et $a - c \equiv b - d\,[n]$
- $ac \equiv bd\,[n]$
- $a^p \equiv b^p\,[n]$ pour tout $p \in \mathbb{N}$

**C'est en 1801 que Carl Friedrich Gauss a introduit la notion de congruence et le symbole $\equiv$**

## A retenir

**Définition**

Soit $n$ un entier naturel non nul, $a$ et $b$ deux entiers relatifs.
On dit que $a$ et $b$ sont **congrus modulo *n*** lorsque $a$ et $b$ ont le même reste dans la division euclidienne par $n$. On note : $a \equiv b$ (modulo $n$) ou $a \equiv b\,[n]$

**Théorème**

Soit $n$ un entier naturel non nul, $a$ et $b$ deux entiers relatifs. On a :
$a \equiv b\,[n]$ si, et seulement si, $a - b$ **est multiple de *n***.

**Remarque**

• $n$ étant un entier naturel non nul, si $r$ est le reste dans la division euclidienne de $a$ par n alors $a \equiv r\,[n]$ mais une relation $a \equiv r\,[n]$ ne permet de conclure que $r$ est le reste dans la division euclidienne de $a$ par $n$ que dans le cas où $0 \leq |n|$

**Propriétés**

Soient $n$ un entier naturel non nul et $a, b, c, d$ des entiers relatifs.

1) $a \equiv a\,[n]$

2) Si $a \equiv b\,[n]$ alors $b \equiv a\,[n]$ .

3) Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ alors $a \equiv c\,[n]$ .

4) Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$ alors $a + c \equiv b + d\,[n]$ et $a - c \equiv b - d\,[n]$ .

5) Si $a \equiv b \ [n]$ et $c \equiv d \ [n]$ alors $a \times c \equiv b \times d \ [n]$.

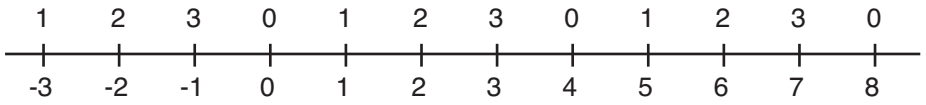
6) Si $a \equiv b \ [n]$ alors $a^p \equiv b^p \ [n]$ pour tout $p \in \mathbb{N}$

**Remarque**

Pour l'addition, la soustraction et la multiplication les règles de calculs sur les égalités se transmettent aux congruences.

## Applications

1 Interpréter à l'aide des congruences la représentation suivante :




2 1) Comment écrire par une congruence que $a$ est un multiple de $m$ ?

2) Compléter les congruences suivantes :

$17 \equiv \ldots [5]$ ; $-3 \equiv \ldots [8]$ ; $21 \equiv \ldots [3]$.

3) Les congruences suivantes sont-elles vraies ?

$27 \equiv 37 [3]$ ; $145 \equiv 1315 [5]$ ; $-5 \equiv -4 [2]$.

3 Vérifier que :

$10 \equiv 3 \ [7]$ , $100 \equiv 2 \ [7]$ , $1000 \equiv -1 \ [7]$ , $10000 \equiv -3 \ [7]$ , $100000 \equiv -2 \ [7]$

$1000000 \equiv 1 \ [7]$

En déduire, parmi ces nombres, ceux qui sont multiples de 7 :

4 123 ; 321 083 ; 39 398 ; 1 111 117 ; 3 333 337.

4 Vérifier que $9 \equiv -1 \ [10]$. En déduire le chiffre des unités des nombres $9^{2n}$ et $9^{2n+1}$.

5 1) Montrer que 9 divise $7^{3n} - 1$ pour tout $n$ nombre entier naturel.

2) Démontrer que l'on a : $2 \times 35^{2006} - 3 \times 84^{2007} \equiv 5 [17]$

6 1) Quel est le reste de la division euclidienne par 7 du nombre $32^{45}$ ?

2) Quel est le reste de la division euclidienne par 19 du nombre $57383^{114}$ ?

3) Quel est le reste de la division euclidienne par 7 du nombre $91234^{2007}$ ?

4) Quel est le reste de la division euclidienne de $2006^{2008}$ par 2007 ?

7 $a$ et $b$ ont pour reste 17 et 15 dans la division par 19.

Quel est le reste de $a + b$ , de $ab$ , de $2a - 5b$ , de $a^2 b^3$ par 19 ?

8 1) Prouver par des exemples, qu'en général, lorsque $c$ divise $a$ et $a'$

« $a \equiv a' [n]$ » n'implique pas « $\frac{a}{c} \equiv \frac{a'}{c} [n]$ ».

2) Prouver que si $a, a'$ et $n$ sont divisibles par un même entier $c$,

alors « $a \equiv a' [n]$ » implique « $\frac{a}{c} \equiv \frac{a'}{c} \left[\frac{n}{c}\right]$ ».

## IV. PGCD et PPCM de deux entiers

### Activités préliminaires

#### Activité 1 :

1) Quels sont les diviseurs de 9? de 12?
2) Déterminer $9 \wedge 12$ (plus grand commun diviseur de 9 et 12).
3) Déduire $63 \wedge 84$ puis $63 \wedge 147$ .

#### Activité 2 :

1) Donner les 6 premiers multiples positifs de chacun des entiers 6 et 8.
2) Déterminer $6 \vee 8$ (plus petit commun multiple de 6 et 8)
3) Déduire $30 \vee 240$ puis $210 \vee 240$

### Activités de découverte

#### Activité 1 :

Déterminer les diviseurs de 12 puis les diviseurs de (- 18). En déduire les diviseurs communs à 12 et (-18). Quelle est alors le plus grand commun diviseur de 12 et (-18). Ce nombre est noté **PGCD** (12 ;-18) ou $12 \wedge (-18)$

#### Activité 2:

Soit $a$ et $b$ deux entiers relatifs et $D(a , b)$ l'ensemble des diviseurs communs à ces deux entiers.
1) Démontrer que $D(a, b) = D(a - b, b) = D(a - k b, b)$ pour tout $k \in \mathbb{Z}$ .
2) Si $0 < b \leq a$ , démontrer que $D(a,b) = D(r,b)$, où $r$ est le reste de la division euclidienne de $a$ par $b$ .
3) Si $a$ et $b$ sont tous les deux non nuls, démontrer que $D(a, b)$ admet un plus grand élément d.Ce nombre est le PGCD de a et b . Pourquoi ce nombre est strictement positif ?
Conclure que $PGCD(a, b) = \text{PGCD}(b,a) = PGCD(|a|,|b|)$ ;
donc on se ramène en général à $a$ et $b$ positifs.
4) Chercher $PGCD$ (240,36) en appliquant plusieurs fois de suite la propriété vue dans 2).
5) Si $0 < b \leq a$, démontrer que PGCD $(a, b)$ = PGCD $(b, r)$ où $r$ est le reste de la division euclidienne de $a$ par $b$.

#### Activité 3:

1) Si $a$ et $b$ sont tous les deux non nuls, vérifier que $|a\,b|$ est un multiple commun à $a$ et $b$ .
2) En déduire l'existence d'un plus petit commun multiple, strictement positif, à $a$ et $b$.
Ce nombre se note ***PPCM*** $(a , b)$ *ou* $a \vee b$.
Déduire que $PPCM\ (a, b) = PPCM\ (b, a) = PPCM\ (|a|,|b|)$.

Activité 4 :

Soit $a$ et $b$ deux entiers relatifs non nuls.

1) En écrivant l'algorithme d'Euclide pour la recherche du $PGCD(a, b)$ puis en multipliant les égalités obtenues par un entier relatif non nul $k$, montrer que :

$$PGCD(k\,a, k\,b) = |k|\, PGCD(a, b).$$

2) a) Montrer que si $d = PGCD(a, b)$ alors il existe $a'$ et $b'$ deux entiers premiers entre eux (c'est-à -dire $a' \wedge b' = 1$) tels que $a = da'$ et $b = d\,b'$.

b) Montrer que si $a = da'$ et $b = d\,b'$ avec $a' \wedge b' = 1$ et $d > 0$ alors $a \wedge b = d$.

la propriété démontrée en 2) est **la propriété caractéristique** du $PGCD$. Enoncer cette propriété.

## A retenir

### Définitions

Soient $a$ et $b$ deux entiers relatifs non nuls.

1) Le plus grand entier qui divise à la fois $a$ et $b$ s'appelle **le plus grand commun diviseur** ou **PGCD** de $a$ et $b$ . On le note $a \wedge b$ .

2) Le plus petit entier strictement positif qui est à la fois multiple de $a$ et $b$ s'appelle **le plus petit commun multiple** ou **PPCM** de $a$ et $b$ . On le note $a \vee b$

3) Deux entiers relatifs non nuls $a$ et $b$ sont **premiers entre eux** lorsque leur PGCD est égal à 1.

### Propriétés

1) Soient $a$ et $b$ deux entiers relatifs non nuls.

Pour tout $k$ entier relatif non nul, $PGCD(k\,a, k\,b) = |k|\, PGCD(a, b)$.

2) Soit $a$ et $b$ deux entiers relatifs non nuls et $d$ un entier naturel non nul.

$d = PGCD(a, b)$ si, et seulement si, $a = da'$ et $b = db'$ avec $a'$ et $b'$ entiers premier entre eux.

### L'algorithme d'Euclide

Le résultat suivant permet de calculer $d = PGCD(a, b)$ sous forme algorithmique.

Soit $a$ et $b$ deux entiers naturels non nuls. Considérons la suite des divisions euclidiennes :

- de $a$ par $b$ : $a = bq_0 + r_0$
- de b par $r_o$ (si $r_0 \neq 0$) : $b = r_0 q_1 + r_1$
- de $r_o$ par $r_1$ (si $r_1 \neq 0$) : $r_0 = r_1 q_2 + r_2$
- de $r_{n-1}$ par $r_n$ (si $r_n \neq 0$) : $r_{n-1} = r_n q_{n+1} + r_{n+1}$

Lorsque $b$ ne divise pas $a$, le $PGCD$ de $a$ et $b$ est le **dernier reste non nul** obtenu par cet algorithme.

Si $b$ divise $a$ alors $PGCD(a,b) = b$.

### Remarque

Pour $b \neq 0$ $PGCD(1,b) = 1$ et , $PGCD(0,b) = |b|$

Si $a$ et $b$ sont deux entiers non nuls tels que $b$ divise $a$ alors PPCM( $a$ , $b$) = $|a|$

1 Dans chaque cas, déterminer le PGCD, puis le PPCM des entiers $a$ et $b$ par une méthode au choix.
a) $a = 35$ et $b = 84$ ; b) $a = 39$ et $b = 52$ ; c) $a = -60$ et $b = 45$ ; d) $a = 18$ et $b = -12$.

2 A l'aide de l'algorithme d'Euclide, déterminer $a \wedge b$.
a) $a = 441$ et $b = 777$ ; b) $a = 2007$ et $b = 9185$ ; c) $a = 1600$ et $b = 259$ .

3 Les entiers suivants sont-ils premiers entre eux ?
a) $a = 4847$ et $b = 5633$ b) $a = 5617$ et $b = 813$

4 Soit $a$ et $b$ deux entiers non nuls.Sachant que $a \wedge b = b \wedge (a - b)$ . Calculer par cette méthode $1575 \wedge 210$.

## V. Théorème de Bézout

### Activités de découverte

Activité 1 :

1) Ecrire l'algorithme d'Euclide pour déterminer $PGCD(145,55)$.
2) En partant de la dernière égalité où le reste est non nul et en exprimant celui-ci successivement en fonction des restes précédents,déterminer un couple (u;v) d'entiers relatifs tels que : $145u + 55v = PGCD(145,55)$.


E Bézout

Activité 2 :

Soit $a$ et $b$ deux entiers relatifs non nuls et $d$ leur $PGCD$.
Considérons l'ensemble $G$ des entiers naturels non nuls de la forme $(am + bn)$ (avec $m$ et $n$ dans $\mathbb{Z}$ ).
1) Vérifier que $|a| \in G$ . En déduire que $G$ admet un plus petit élément $D$.
Il existe alors $u$ et $v$ deux entiers relatifs tels que $au + bv = D$ .
2) Montrer que $d$ divise $D$, en déduire que $d \leq D$.
3) La division euclidienne de $a$ par $D$ s'écrit $a = Dq + r$ avec $0 < r < D$.
Exprimer $r$ en fonction de $a$ ,$b$ , $u$, $v$ et $q$. En déduire que $r$ est de la forme $am + bn$ .
4) Déduire que $r = 0$ et que $D$ divise $a$ .
5) On montre de façon analogue que $D$ divise $b$ . Déduire que $D = d$

Activité 3 :

Soit $a$ et $b$ deux entiers relatifs non nuls. En utilisant le résultat de l'activité 2 démontrer que
1) Tout diviseur commun à $a$ et $b$ divise leur $PGCD$.

2) $a$ et $b$ sont premiers entre eux si, et seulement si, il existe deux entiers relatifs $u$ et $v$ tels que $au + bv = 1$

3) L'équation $ax + by = c$ ($c$ entier fixé non nul) admet des solutions entières si, et seulement si $c$ est un multiple de $PGCD\ (a,b)$ .

## A retenir

**Théorème**

$a$ et $b$ désignent deux entiers relatifs non nuls et $d$ leur $PGCD$. Il existe deux entiers relatifs $u$ et $v$ tels que $au + bv = d$ .

**Théorème de Bézout**

$a$ et $b$ désignent deux entiers relatifs non nuls. $a$ et $b$ sont premiers entre eux si, et seulement si, il existe deux entiers relatifs $u$ et $v$ tels que :

$$au + bv = 1.$$

L'égalité $au + bv = 1$ s'appelle **relation de Bézout** (ou identité de Bézout *)

**Remarque**

Le théoréme de Bézout est un théorème d'existence mais pas d'unicité.

**Conséquences**

Soit $a$ et $b$ deux entiers relatifs non nuls

1) tout diviseur commun à $a$ et $b$ divise leur $PGCD$.

2) l'équation $ax + by = c$ ($c$ entier fixé non nul) admet des solutions entières si, et seulement si $c$ est multiple de $PGCD\ (a, b)$ .

***Ce théorème fut en fait énoncé pour les entiers par Bachet de Méziriac (1581-1638), mais fut ensuite démontré et utilisé dans d'autres domaines par Etienne Bézout (1730-1783).**

## Applications

1 Pour déterminer les entiers relatifs $u$ et $v$ tels que $au + bv = 1$ quand $a$ et $b$ sont premiers entre eux, l'examen rapide des multiples de $a$ et $b$ peut permettre de conclure, sinon, on écrit l'algorithme d'Euclide pour $a$ et $b$ , puis on exprime pas à pas chacun des restes comme combinaison linéaires de $a$ et $b$ , jusqu'au dernier reste non nul qui est PGCD($a$, $b$).

Ce procédé permet d'exprimer $PGCD(a, b)$ comme combinaison linéaire de $a$ et $b$, que $a$ et $b$ soient premiers entre eux ou non.

On utilise ci-dessous l'algorithme d'Euclide pour déterminer $212 \wedge 87$

Etape 1 : $212 = 2 \times 87 + 38$

Etape 2 : $87 = 2 \times 38 + 11$

Etape 3 : $38 = 3 \times 11 + 5$

Etape 4 : $11 = 2 \times 5 + 1$

Etape 5 : $5 = 5 \times 1$

1) De l'étape1, déduire $u_2 \in \mathbb{Z}$ et $v_2 \in \mathbb{Z}$ tels que $38 = au_2 + bv_2$

2) De l'étape 2, déduire $u_3 \in \mathbb{Z}$ et $v_3 \in \mathbb{Z}$ tels que $11 = au_3 + bv_3$

3) De l'étape 3, déduire $u_4 \in \mathbb{Z}$ et $v_4 \in \mathbb{Z}$ tels que $5 = au_4 + bv_4$

4) De l'étape 4, déduire $u_5 \in \mathbb{Z}$ et $v_5 \in \mathbb{Z}$ tels que $1 = au_5 + bv_5$

2 Pour $a = 4$ et $b = 9$, vérifier que les couples $(-2\ ;1)$ ; $(7\ ;-3)$ ; $(97\ ;-43)$ sont tous des couples $(u\ ;v)$ vérifiant l'égalité $au + bv = 1$.

3 Démontrer que les entiers $a$ et $b$ sont premiers entre eux, où $n$ est un entier.

a) $a = n$ ; $b = 2n + 1$ b) $a = 2n + 3$ ; $b = 3n + 5$ c) $a = n^2 + 1$ ; $b = n$

4 $n$ désigne un entier naturel non nul.

1) Vérifier que $(n^3 + 1)^2 = n^2(n^4 + 2n) + 1$

2) En déduire que les entiers naturels $n^3 + 1$ et $n^4 + 2n$ sont premiers entre eux

5 Utiliser l'algorithme d'Euclide pour déterminer une solution particulière $(x_0\ ,\ y_0)$ d'entiers relatifs de chaque équation :

a) $726x + 137y = 1$ b) $2017x + 1771y = 1$

## VI. Lemme de Gauss

### Activités de découverte

C . F Gauss
( 1777 - 1855)

Activité 1 :

Soient $a, b$ et $c$ trois entiers relatifs non nuls.
On suppose que $a$ divise $bc$ et $a$ est premier avec $b$.

1) Montrer qu'il existe $k \in \mathbb{Z}$ , tel que $bc = ka$.

2) Montrer qu'il existe $u$ et $v$ dans $\mathbb{Z}$ , tel que $c = a\,(cu + kv)$ .
En déduire que $a$ divise $c$.

3) Enoncer alors ce résultat établi par Gauss.

Activité 2 :

En utilisant le résultat précédent, démontrer les propriétés suivantes :

1) Si $a$ et $b$ divisent un entier $c$, et si $a$ et $b$ sont premiers entre eux alors ***ab* divise *c*.**

2) Si un entier $a$ est premier avec chacun des entiers $b_1, b_2, \ldots, b_k$ alors $a$ **est premier** avec leur produit $b_1\ b_2 \ldots b_k$ .

Activité 3 :

Soient $a$ et $b$ deux entiers relatifs non nuls, $d$ leur *PGCD* et $m$ leur *PPCM*.

1) Justifier que $a = da'$ et $b = db'$ avec $a'$ et $b'$ des entiers premiers entre eux .

2) Montrer que $da'b'$ est un multiple commun à $a$ et $b$.
3) Soit $M = ka = k'b$ un autre multiple commun à $a$ et $b$, ($k$ et $k'$ sont des entiers relatifs). En exprimant $M$ en fonction de d, $a'$ et $b'$, montrer que $ka' = k'b'$ puis déduire que $a'$ divise $k'$.
4) Exprimer alors $M$ en fonction de $da'b'$ et déduire que tout multiple commun à $a$ et $b$ est un multiple de $da'b'$. En déduire que $m = d|a'b'|$ .
5) Exprimer $PGCD(a,b) \times PPCM(a,b)$ en fonction de $a$ et $b$.

Activité 4 :

Soit $a$ et $b$ deux entiers relatifs non nuls, $d$ leur $PGCD$ et $m$ leur $PPCM$.
1) Utiliser l'identité de Bézout pour monter que l'ensemble des diviseurs communs à $a$ et $b$ est l'ensemble des diviseurs de $d$.
2) Prouver que l'ensemble des multiples communs à $a$ et $b$ est l'ensemble des multiples de $m$
3) En utilisant la relation entre PGCD et PPCM de deux entiers $a$ et $b$, montrer que pour tout entier relatif non nul $k$, on a : $(ka \vee kb) = |k|\ (a \vee b)$.

## A retenir

### Lemme de Gauss

Soit $a$, $b$ et $c$ trois entiers relatifs non nuls.
Si ***a* divise *b.c*** et si ***a* et *b* sont premiers entres eux**, alors ***a* divise *c*.**

### Propriétés

Soit a et b deux entiers relatifs non nuls, alors on a :
1) $(a \wedge b)(a \vee b) = |ab|$ .
2) $(ka \vee kb) = |k|(a \vee b)$.
3) L'ensemble des diviseurs communs à $a$ et $b$ est l'ensemble des diviseurs de $a \wedge b$
4) L'ensemble des multiples communs à $a$ et $b$ est l'ensemble des multiples de $a \vee b$

## Applications

1 Dans chacun des cas suivants, déterminer $d = a \wedge b$ à l'aide de l'algorithme d'Euclide, puis $m = a \vee b$.
a) $a = 576$ et $b = -480$ ; b) $a = 225$ et $b = 350$ ; c) $a = -845$ et $b = -234$.

2 Soit $a$ et b deux entiers premiers entre eux.
a) Démontrer que, pour tous $m$ et $n$ dans IN, $a^m$ et $b^n$ sont premiers entre eux.
b) Si $d$ et $d'$ sont des diviseurs respectifs de $a$ et $b$, montrer que $d$ et $d'$ sont premiers entre eux.

3 Prouver le résultat suivant : lorsque $x$ et $n$ sont premiers entre eux, alors
$a\,x \equiv a'x\,[n]$ implique $a \equiv a'\,[n]$ .

## VII. application : résolution dans $\mathbb{Z} \times \mathbb{Z}$ d'équations du type $ax + by = c$ où $a$, $b$ et $c$ sont des entiers relatifs

### Activités de découverte

$x$ et $y$ désignent des entiers relatifs.

1) Pourquoi l'équation $37x + 27y = 1$ admet-elle des solutions dans $\mathbb{Z} \times \mathbb{Z}$ ?

2) En utilisant l'algorithme d'Euclide donner une solution particulière de cette équation.

3) En déduire une solution particulière $(x_o;y_o)$ dans $\mathbb{Z} \times \mathbb{Z}$ de l'équation

$$(E) : 37x + 27y = 1000.$$

4) Démontrer que toute solution $(x;y)$ de $(E)$ dans $\mathbb{Z} \times \mathbb{Z}$ vérifie : $37(x-x_o) = -27(y-y_o)$.

5) En utilisant le théorème de Gauss, démontrer que si $(x;y)$ est une solution de $(E)$ alors il existe $k \in \mathbb{Z}$ tel que $\begin{cases} x = x_0 + 27k \\ y = y_0 - 37k \end{cases}$

6) En déduire l'ensemble des solutions de $(E)$.

**Méthode de résolution**, dans $\mathbb{Z} \times \mathbb{Z}$, de l'équation $ax + by = c$ où $a$, $b$ et $c$ sont des entiers relatifs.

1) On détermine $d = PGCD(a,b)$.

2) Si $c$ n'est pas un multiple de $d$, on en déduit que l'équation n'a pas de solutions entières. Sinon, on divise $a$, $b$ et $c$ par $d$. on obtient alors une équation de la forme $Ax + By = C$, avec $A$ et $B$ premiers entre eux.

3) On détermine une solution particulière $(u, v)$ de l'équation. Pour cela, on peut déterminer une solution particulière de l'équation $ax + by = d$ ( équivalente à $Ax + By = 1$ ) à l'aide de l'algorithme d'Euclide et multiplier les nombres obtenus par $\frac{c}{d} = C$.

4) On écrit $\begin{cases} Ax + By = C \\ Au + Bv = C \end{cases}$

En soustrayant membre à membre, on obtient l'équation : $A(x-u) = -B(y-v)$.

$A$ et $B$ étant premiers entre eux, d'après le théorème de Gauss, $y-v = kA$

d'où par substitution $x- v = - k B$.

Finalement l'ensemble des solutions est l'ensemble des couples de la forme : $(u-kB;v+kA)$où $k$ désigne un entier relatif arbitraire.

**Exercice résolu** : Soit l'équation $(E)$ $62x + 43y = 1$.

1) On va écrire l'algorithme d'Euclide avec les entiers 62 et 43 :

$62 = 43 \times 1 + 19$ (4)

$43 = 19 \times 2 + 5$ (3)

$19 = 5 \times 3 + 4$ (2)

$5 = 4 \times 1 + 1$ (1)

On remarque que, d'après la dernière égalité, PGCD(62,43) = 1, donc l'équation $(E)$ admet des solutions (théorème de Bézout).

2) Une solution particulière de $(E)$ :

On va déterminer une solution particulière en remontant les égalités (1), (2), (3) et (4) dans l'algorithme, et en éliminant les restes successifs sauf le PGCD.

(1) donne $5 = 4 \times 1 + 1$ (1') ;
l'étape 2 consiste à éliminer le reste 4 dans (2).
Comme (1') contient le produit $4 \times 1$, on multiplie (2) par 1 :
$19 \times 1 = 5 \times 3 + 4 \times 1 = 5 \times 3 + 5 - 1$. On obtient $19 \times 1 = 5 \times 4 - 1$ (2').
A l'étape 3, il s'agit d'éliminer le reste 5 dans (3). Comme (2') contient le produit $5 \times 4$,
on multiplie (3) par 4 : $43 \times 4 = 19 \times 8 + 5 \times 4 = 19 \times 8 + 19 \times 1 + 1$.
d'après (2'), on obtient $43 \times 4 = 19 \times 9 + 1$ (3').
Etape 4 : il s'agit d'éliminer le reste 19 dans (4). Comme (3') contient le produit $19 \times 9$,
on multiplie (4) par 9 : $62 \times 9 = 43 \times 9 + 19 \times 9 = 43 \times 9 + 43 \times 4 - 1$.
D'après (3'). on obtient $62 \times 9 = 43 \times 13 - 1$ (4').
Conclusion : $62 \times (-9) + 43 \times 13 = 1$, donc $(-9 ; 13) = (x_o ; y_o)$ est une solution particulière de $(E)$.

3) Solution générale de $(E)$ :
L'équation (E) équivaut à : $62x + 43y = 62x_o + 43y_o$ ;
soit encore : $62(x - x_o) = 43(y - y_o)$ (E ').
62 doit diviser $43(y - y_o)$ ; or 62 est premier avec 43, donc 62 doit diviser $y - y_o$
(lemme de Gauss).
On établit de même que 43 doit diviser $x - x_o$ . Ainsi il existe $k$ et $l$ entiers tels que :

$$y - y_o = 62k \text{ et } x - x_o = 43l .$$

Puisque (E') s'écrit $62 \times 43 l = 43 \times 62 k$ , on en tire $l = k$ .
conclusion : $x = x_o + 43k = -9 + 43k$ et $y = y_o - 62k = 13 - 62k$ .
réciproquement, il est clair que ces valeurs sont solutions de $(E)$.

**Applications**

Déterminer tous les couples d'entiers relatifs solutions des équations suivantes :

a) $10x+13y = 1$ b) $42x+35y = 7$ c) $120x+26y = 2$ d) $39x-52y = 3$

## Situation 1 : Résolution de l'équation $a\,x \equiv b$ (modulo $n$)

$a,b,n$ sont trois entiers donnés, $n > 0$, cherchons à résoudre dans $\mathbb{Z}$, l'équation d'inconnue $x$ :

$$a\,x \equiv b \text{ (modulo } n\text{)}.$$

1) Démontrer que s'il existe une solution $x$ , alors $a \wedge n$ divise $b$ .

2) Réciproquement, prouver que si $a \wedge n$ divise $b$ , alors l'équation $ax \equiv b$ (modulo $n$), a une solution.

3) On se propose de résoudre la congruence $(C)$ : $9x \equiv 15$ ( modulo 24)

a) Justifier l'existence d'une solution de $(C)$

b) Vérifier que $9x \equiv 15$ (modulo 24) $\Leftrightarrow 3x \equiv 5$( modulo 8).

c) Prouver que $3x \equiv 5$ (modulo 8) $\Leftrightarrow x \equiv 7$(modulo 8) (on justifiera la condition nécessaire puis la condition suffisante)

d) En déduire l'ensemble de solutions de $(C)$

4) Résoudre, dans $\mathbb{Z}$ , les congruences : $6x \equiv 6$ (modulo 21); $-3x \equiv 15$ (modulo 13).

## Situation 2 : Critères usuels de divisibilité

Rappelons que tout entier naturel s'écrit : $a = a_n 10^n + a_{n-1}10^{n-1} + \ldots + a_2 10^2 + a_1 10 + a_0$
où chaque $a_i$ désigne un nombre entier compris entre 0 et 9 et $a_n \neq 0$

### 1. Critère de divisibilité par 9

a) Justifier les résultats suivants :

$10 \equiv 1$(modulo 9) et pour tout entier naturel $n$, $10^n \equiv 1$ (modulo 9).

Si $a = a_n 10^n + a_{n-1}10^{n-1} + \ldots + a_2 10^2 + a_1 10 + a_0$ alors $a \equiv a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 \,[9]$

b) Déduire le critère suivant : un entier est divisible par 9 si et seulement si la somme de ses chiffres est un multiple de 9.

### 2. Critère de divisibilité par 3

En procédant comme ci-dessus, prouver le Critère suivant : *un entier est divisible par 3 si et seulement si la somme de ses chiffres est un multiple de 3.*

### 3. Critère de divisibilité par 4, par 25

Prouver les critères suivants : *un entier est divisible par 4 (resp. par 25) si et seulement si le nombre formé par les deux derniers chiffres est divisible par 4 (resp. par 25).*

### 4. Critère de divisibilité par 8, par 125

Trouver un critère de divisibilité par 8, et un critère de divisibilité par 125.

### 5. Critère de divisibilité par 11

a) Justifier les résultats suivants :

Lorsque $n$ est pair, $10^n \equiv 1$ (modulo 11), et lorsque $n$ est impair, $10^n \equiv -1$ (modulo 11).

b) En procédant comme dans 1. prouver le critère suivant : *un entier naturel est divisible par 11 si et seulement si la différence entre la somme des chiffres de rang impair et la somme des chiffres de rang pair à partir de la droite est un multiple de 11.*

c) Le nombre 4 792 178 est-il divisible par 11 ?

### 6. Critère de divisibilité par 7

a) Soit $n$ un entier naturel qui s'écrit : $n = 10a + b$ ($a,b$ dans $\mathbb{N}$ ).
Vérifier que $n = 7(a + b) + 3(a - 2b)$ et déduire que $n$ est divisible par 7 si, et seulement si, $a - 2b$ est divisible par 7.

b) Sans calculatrice, déterminer les nombres divisibles par 7 parmi 25 718 ; 62 216 ; 46 663 et 38 983.

1. Etudier les restes, dans la division euclidienne, de $3^n$ par 11.

| | A | B | C | D |
|---|---|---|---|---|
| 1 | | | Restes de a^n par b | |
| 2 | | | a | b |
| 3 | Zone de saisie: | | 3 | 11 |
| 4 | | n | a^n | Restes |
| 5 | | 0 | 1 | 1 |
| 6 | | 1 | 3 | 3 |
| 7 | | 2 | 9 | 9 |
| 8 | | 3 | 27 | 5 |
| 9 | | 4 | 81 | 4 |
| 10 | | 5 | 243 | 1 |

Les quatre premières lignes sont de la présentation; les formules se trouvent sur la ligne 5, colonne *C* et *D*. Ces sont respectivement : =$C$3^B5 et =MOD(C5 ;$D$3). Ensuite on recopie vers le bas les deux formules aussi loin que l'on veut en vue de déceler une périodicité.
***Remarque :*** la présentation permet de faire des simulations en changeant les valeurs de *a* et *b* dans la zone de saisie, ce qui permet de résoudre d'autres problèmes.

2. Faites tourner ce programme, en Turbo Pascal, pour obtenir le PGCD des nombres
*a* = 16 170 et *b* = 9450 puis *a* = 195 728 et *b* = 178 211.

```
Program euclide ;
var r,t,q,z :longint ;
begin
Writeln(' Donner a') ;readln(r) ;
Writeln('Donner  b') ;readln(t) ;
 repeat
 q:=r div t;
 z :=r ;r :=t ;t :=z-q*t
 until t=0 ;
 Writeln('Le PGCD est' ,r) ;
end.
```

**3. Algorithme de calcul de coefficients u et v dans la relation de Bézout**
Soit a et b deux entiers naturels non nuls. On note $r_0, r_1, \ldots, r_n, r_{n+1}$, les restes successifs de l'algorithme d'Euclide appliqué aux entiers *a* et *b* ($r_n = PGCD(a,b)$, $r_{n+1} = 0$).
a) Montrer que, pour tout $k$ ($0 \le k \le n$), il existe deux entiers $u_k$ et $v_k$ tels que $au_k + bv_k = r_k$ définir $u_k$ et $v_k$ par récurrence.
b) Programmer le calcul de $u_k$ et $v_k$ sur un tableur. En déduire une solution particulière de l'équation $ax + by = D$ , ( $D$ = PGCD ($a$ , $b$ )) .
**Calcul pratique des suites $(u_k)$ et $(v_k)$**

1) Sur le tableur excel ci-dessous nous avons organisé et présenté les calculs de la manière suivante :

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | a | b | quotient q(k) | restes r(k) | u(k) | v(k) |
| 2 | 78 | 35 | 2 | 8 | 1 | -2 |
| 3 | | | 4 | 3 | -4 | 9 |
| 4 | | | 2 | 2 | 9 | -20 |
| 5 | | | 1 | 1 | -13 | 29 |
| 6 | | | 2 | 0 | | |
| 7 | | | | | | |

Formules utilisées

• Initialisation (k=0 et k=1)

En C2 : = **QUOTIENT (A2 ;B2)**
En D2 : = **MOD ( A2 ;B2)**
En E2 : 1
En F2 : = **- C2**
En C3 : = **QUOTIENT (B2 ;D2)**
En D3 : = **MOD(B2 ; D2)**
En E3 : = **SI (D3=0 ; ‘ ‘ ; - C3)**
En F3 : = SI (D3=0 ; “ “ ; 1+C2*C3)
En C4 : = **SI( D3=0 ; ‘ ‘ ; QUOTIENT (D2 ;D3))**
En D4 : = **SI( D3=0 ; ‘ ‘ ; MOD (D2 ;D3))**
En E4 : = **SI (D4=0 ; ‘ ‘ ; E2-C4*E3)**
En F4 : = **SI (D4=0 ; ‘ ‘ ; F2-C4*F3)**

• Relations de récurrence

Ces relations sont étendues vers le bas, aussi loin que l'on veut.

2) En turbo Pascal

```
program coef_ besout
var
  u,v,r,u1,r1,q,a,b,z :longint ;
begin
  writeln('Donner la valeur du 1er nombre a') ;readln(a) ;
  writeln('Donner la valeur du 2e  nombre b') ;readln(b) ;
  u :=1 ;u1 :=0 ;v1 :=1 ;r :=a ;r1 :=b ;
  while r1< >0 d0
  begin
    q :=rdivr1 ;
    z :=u ;u :=u1;u1:=z-q*u1;
    z:=v;v:=v1;v1:=z-q*v1;
    z:=r;r:=r1;r1:=z-q*r1;
    end;
    writeln('u=',u,'v=',v);
end.
```

▸ z variable intermédiaire pour ne pas perdre u.

# Exercices et problèmes



**1** Vrai ou Faux

Justifier chaque affirmation, par une démonstration ou présenter un contre exemple.

**a)** Un entier divisible par 4 et 15 est aussi divisible par 60.

**b)** Si les entiers $m$ et $n$ vérifient $1111m = 1515n$, alors $m$ est un multiple de 1515

**c)** Le PGCD de $2001^{2007}$ et de $2007^{2001}$ est $3^{1995}$

d) Le reste de la division de $2^{100}$ par 11 est égal à 1.

**e)** Les suites $(u_n)$ et $(v_n)$ sont définies par :

$$u_0 = 3 \text{ et } u_{n+1} = 2u_n - 1;$$
$$v_0 = 1 \text{ et } v_{n+1} = 2v_n + 3$$

Les termes de chaque suite ayant le même indice impair ont pour PGCD 5.

**f)** Il existe un entier $k$ tel que $36^{36}$ soit de la forme $37k + 1$.

**g)** Si a et b sont deux entiers naturels vérifiant la relation $27^a = 3 \times 3^b$ alors les deux entiers $a$ et $b$ sont premiers entre eux.

**h)** Si $a$, $b$ et $c$ sont des entiers naturels tels que c divise $ab$ avec $a$ premier, alors $c$ divise $b$.

i) Si le PPCM de deux entiers naturels est égal à leur produit, alors ils sont premiers entre eux.

**QCM**

**2** Indiquer les réponses justes pour chaque question.

**a)** $x$ et $y$ sont des entiers naturels vérifiant

$$2007x - 19y = 1$$

Le nombre de solutions telles que $x$ et $y$ soient simultanément inférieurs à 1000 est

*a.* 0 ; *b.* 1 ; *c.* 53 ; *d.* 152

**b)** Un terrain rectangulaire, dont les dimensions en mètres sont des nombres entiers de PGCD 6, a pour aire 3024 m². Le nombre de valeurs possibles pour le périmètre est égal à :

*a.* 3 ; *b.* 4 ; *c.* 5 ; *d.* 6.

**c) a.** Si les entiers $a$, $b$, $a'$, et $b'$ vérifient $ab' - a'b = 1$, alors les fractions $\frac{a}{b}$ et $\frac{a'}{b'}$ sont irréductibles.

**b.** Si les entiers $a$, $b$, $a'$, et $b'$ vérifient $ab' - a'b = 2$, alors les fractions $\frac{a}{b}$ et $\frac{a'}{b'}$ sont irréductibles.

**c.** Si les fractions $\frac{a}{b}$ et $\frac{a'}{b'}$ ne sont pas irréductibles alors les entiers $a$, $b$, $a'$, et $b'$ ne vérifient pas $ab' - a'b = 1$.

**d.** Le PGCD de deux nombres entiers a et $b$ est 12 ; les quotients successifs obtenus dans le calcul de ce PGCD par l'algorithme d'Euclide sont 8, 2 et 8. le plus grand de ces nombres est égal à :

A. 1524 ; B. 1728 ; C. 2007.

**e.** Sachant que $123 \equiv 0$ ( modulo 3) alors

**a**. $123^{2005} - 1$ est divisible par 3.

**b**. $124^{2006} - 1$ est divisible par 3.

**c**. $125^{2007} - 1$ est divisible par 3.

**3** Quel est le reste dans la division par 7 des nombres

99988877766655544433322211?

999888777666555444333222111000 ?

**4** Démontrer que, quel que soit l'entier $n \geq 1$

**a)** $3^{2n+1} + 2^{n+2}$ est divisible par 7.

**b)** $3^{2n} + 2^{6n-5}$ est divisible par 11.

**c)** $3.5^{2n-1} + 2^{3n-2}$ est divisible par 17.

**5** 1) Montrer que, pour tout entier $n \in \mathbb{N}$, $n^3 + 5n$ est un multiple de 6.

2) En déduire que les entiers suivants sont multiples de 6 : $n^3 + 17n - 12$ ; $n^3 + 2009n$

**6** 1) Soit $n$ un entier naturel non nul, et $d$ un diviseur positif de $n$. Montrer que, pour tout entier $a \geq 1$, $a^n - 1$, est divisible par $a^d - 1$.

2) Montrer que $2^{2008} - 1$ est divisible par 3, 15 et 255.

**7** Soit $a$, $b$ et $d$ trois entiers naturels. Démontrer que si $7a + 5b$ et $4a + 3b$ sont de multiples de $d$ alors les nombres $a$ et $b$ sont des multiples de $d$.

**8** Déterminer les entiers relatifs $x$ tels que :
**a)** $x - 2$ divise $x + 5$ ;
**b)** $x + 7$ divise $2x + 15$ ;
**c)** $x - 1$ divise $x^2$ ;
**d)** $x + 1$ divise $x^3 + 2$ .

**9** Le dividende d'une division euclidienne est inférieur à 900. Le quotient est 72 et le reste 12. On cherche le diviseur et le dividende. Expliquer pourquoi il n'y a pas de solution

**10** $a$ et $b$ sont deux entiers naturels. Les restes de la division euclidienne de $a$ et $b$ par 11 sont respectivement 2 et 7. Déterminer le reste de la division euclidienne des nombres $a + b$ et $a - b$ par 11. En déduire celui de $a^2 - b^2$ .

**11** **1)** Vérifier que 20072007 est divisible par 137 et 73. En est-t-il de même pour 20082008 ?
**2)** Choisir un nombre de quatre chiffres et le juxtaposer avec lui-même pour obtenir un nombre de huit chiffres. Est-il lui aussi divisible par 137 et 73 ?. Calculer 137 x 73 et justifier le phénomène observé.

**11** **1) a)** Vérifier que l'équation $2x^2 - 2x + 1 = 0$ n'admet pas de solution réelle.
**b)** Vérifier que -21, -13, 34, 112 sont solutions de l'équation :
**(1)** $2x^2 - 2x + 1 \equiv 0$ (modulo 5).
**2) a)** Justifier que $x$ est solution de (1) si et seulement si il existe un entier $k$ tel que :
$2x^2 - 2x + 1 - 5k = 0$ . (2)
**b)** Calculer le discriminant de cette dernière équation. Démontrer que pour que (2) admette une solution entière, il faut qu'il existe un entier $p$ tel que : $p^2 + 1 \equiv 0$ ( modulo 10).
En utilisant les congruences modulo 10, déterminer les entiers $p$ vérifiant la relation ci-dessus.
**c)** Déterminer toutes les solutions de (1).
**3)** Vérifier que les termes des suites arithmétiques de premiers termes -1 et 2 et de raison 5 sont tous solutions de (1).

**13** Vérifier les congruences :
$2^{13} \equiv 1[13]$ et $3^6 \equiv 1[13]$.
En déduire que $2^{70} + 3^{70}$ est divisible par 13.

**14** Vérifier que $7^2 \equiv -1$ (modulo 10).
b) Quel est le chiffre des unités de l'entier naturel :
$1 + 7 + 7^2 + ... + 7^{400}$ ?

**15** $a$, $b$ sont des entiers relatifs et $c$ un entier $> 0$.
Démontrer que si $a \equiv b[c]$ alors
PGCD ($a$ , $c$ ) = PGCD ( $b$ , $c$ ).
La réciproque est-elle vraie?

**16** Pour la proposition suivante, indiquer si elle est vraie ou fausse et donner une démonstration de la réponse choisie.
Si un entier relatif $x$ est solution de l'équation $x^2 + x \equiv 0$ ( modulo 6) alors $x \equiv 0$ (modulo3)

**17** Déterminer les restes possibles dans $\mathbb{Z}$ la division euclidienne par 8 du carré d'un entier.
Déterminer les entiers $n$ dans $\mathbb{Z}$ tels que :
$(n + 3)^2 \equiv 1[8]$

**18** Expliquer, sans nécessairement calculer les PGCD, pourquoi tous les résultats suivants sont visiblement faux :
**a)** PGCD (1602; 1846) =3
**b)** PGCD (1714; 3026) =1
**c)** PGCD (15; 23) =7
**d)** PGCD (132; 63) = 63
**e)** PGCD (2121; 111) = 140
**f)** PGCD (121; 128) = 8

**19** Trouver les nombres entiers naturels non nuls $a$ et $b$ de PGCD égal à 8 et tels que $a+b = 144$.

**20** $n$ est un entier naturel non nul ; $a = 2n^2$ et $b = n(2n+1)$. justifier que $2n$ et $2n+1$ sont premiers entre eux. En déduire le PGCD de $a$ et $b$.

**21** $a$ et $b$ sont des entiers naturels. Trouver $a$ et $b$ sachant que $ab = 1734$ et que le PGCD de $a$ et $b$ est 17.

**22** Calculer le PGCD et le PPCM des nombres non nuls $a$ et $b$ définis par :$a = 5^{n+2} - 5^n$ et $b = 7^{n+2} - 7^n$ où $n$ est un entier naturel.

**23** Résoudre dans l'ensemble des entiers naturels les systèmes :

**a)** $\begin{cases} xy = 1512 \\ PPCM(x;y) = 252 \end{cases}$

**b)** $\begin{cases} x + y = 276 \\ PPCM(x;y) = 1440 \end{cases}$

**c)** $\begin{cases} xy = 16128 \\ PGCD(x;y) = 24 \end{cases}$

**24** Résoudre l'équation 2PGCD $(a\ ;\ b) = 111$ où $a$ et $b$ désignent des entiers naturels.

**25** Trouver tous les couples $(a\ ;\ b)$ d'entiers naturels non nuls $(a < b)$ vérifiant :
2PPCM $(a\ ;\ b)$ + 3PGCD $(a\ ;\ b) = 78$
et tels que $a$ ne divise pas $b$.

**26** Soit $a$, $b$ et $n$ des entiers naturels.
**a)** Montrer que si PGCD $(a,b) = 1$, alors PGCD $(a^n\ ,\ b) = 1$
**b)** En déduire :
PGCD $(a,b) = 1 \Rightarrow$ PGCD $(a^n, b^n) = 1$.
**c)** La réciproque est-elle vraie ? Justifier

**27** Déterminer tous les couples d'entiers relatifs $(x\ ;y)$ solutions des équations suivantes :
**a)** 10 x +13y =1 ; b) 5 x + 3y =1
**c)** 30 x +35 y =100 ; d) 9 x - 15 y = 1

**28** On pose, pour $n$ entier relatif $(n \neq 7)$,
$a_n = n + 7$ et $b_n = 3n - 4$
**1)** Calculer $3a_n - b_n$ . En déduire que PGCD $(a_n\ ,\ b_n)$ est un diviseur de 25.
**2)** On pose $d_n = PGCD(a_n, b_n)$
Montrer que $d_n = PGCD(a_n, 25)$
**3)** En déduire les équivalences :
**a)** $d_n = 5 \Leftrightarrow n \equiv 3\,[5]$

**b)** $d_n = 25 \Leftrightarrow n \equiv 18\,[25]$

**4)** En dehors des deux cas précédents, prouver que $a_n$ et $b_n$ sont premiers entre eux.

**29** 1) On désigne par $n$ un nombre entier naturel quelconque. On suppose que $n \equiv 1\,[7]$
**a)** Déterminer un nombre entier naturel $p$ tel que $n^3 \equiv p\ [7]$ .
**b)** En déduire que le nombre entier $n^3 + 1$ est divisible par 7.
**2)** Soit $m$ un nombre entier naturel quelconque. Prouver que si $m \equiv 4$ ( modulo **7)** alors le nombre entier $m^3 - 1$ est divisible par 7.
**3)** On considère le nombre A= $1999^3 + 2007^3$.
**a)** Justifier que $1999 \equiv 4$ ( modulo 7)
**b)** Déterminer le plus petit entier naturel $p$ tel que $2007 \equiv p$ ( modulo 7).
**c)** En déduire, sans calcul, que 7 divise l'entier $A$.

**30** **1)** Soit $n$ un entier naturel qui s'écrit : $n = 10\,a + b$ , avec $a$ et $b$ dans IN .
Prouver que $n$ est divisible par 13 si, et seulement si, $a + 4\,b$ est divisible par 13.
**2)** Application : Sans calculatrice déterminer les nombres divisibles par 13 parmi : 569 556; 8 888 ; 6 666 ; 6 567.

**31** 1) Soit $n$ un entier naturel qui s'écrit : $n = 10a + b$, avec $a$ et b dans $\mathbb{N}$.
Prouver que n est divisible par 17 si, et seulement si, $a - 5b$ est divisible par 17.
2) Application : Sans calculatrice déterminer les nombres divisibles par 17 parmi : 16 831 ; 152 592 ; 16 983 ; 83 521.

**32** Le nombre $2^{11} - 1$ est-t-il premier ?
Si $p$ et $q$ sont deux entiers naturels non nuls, comment la somme :
$S = 1 + 2^p + 2^{2p} + 2^{3p} + ... + 2^{p(q-1)}$
peut-elle encore s'écrire ?
en déduire que $2^{pq} \equiv 1\left[2^p - 1\right]$
Démontrer que $2^{pq} - 1$ est divisible par les deux nombres $2^p$-1 et $2^q$-1. En déduire que si le nombre $2^n - 1$ est premier, alors $n$ est lui-même premier. La réciproque est-elle vraie ?
Les nombres premiers de la forme $2^n - 1$ sont appelés nombres de MERSENNE.

**33** Dans un pays imaginaire, la banque nationale émet seulement des pièces de monnaie de 13 et 4 unités monétaires.
1) Montrer qu'il est possible de payer n'importe quelle somme entière (à condition de disposer d'assez de pièces).
2) Si on ne rend pas la monnaie, quelle est la plus grande somme qu'il est possible de payer?

**34** On dispose sur la table de 38 allumettes. Deux joueurs $A$ et $B$ prennent, chacun à son tour, un nombre d'allumettes compris entre 1 et 4. Le joueur qui prend la dernière allumette a perdu. Le joueur qui commence et qui joue avec une stratégie bien définie, peut gagner la partie à coup sûr. Trouver et justifier cette stratégie.
La stratégie est-elle valable quelque soit le nombre d'allumettes posées sur la table en début de partie ?

**35** Le code ISBN (International Standard Book Number) permet d'identifier chaque livre de manière unique dans le monde entier. Il sert notamment de numéro de référence dans des bases de données informatiques. Il comprend dix chiffres répartis en quatre groupes séparés par des tirets (Exemple : ISBN 9973 - 719 - 55 - 7).
Le premier groupe correspond au pays de l'éditeur, le deuxième groupe est le numéro de l'éditeur, le troisième celui du livre, enfin le dernier chiffre est une clé qui sert à vérifier qu'on n'a pas effectué d'erreur de saisie en rentrant le code dans un ordinateur. Cette clé est calculée de la maniéré suivante $a_1, a_2, a_3, ...a_9$
A partir des neuf premiers chiffres (sans tenir compte des tirets), on calcule la somme $S = a_1 + 2 \times a_2 + 3 \times a_3 + 4 \times a_4 + 5 \times a_5 + 6 \times a_6 + 7 \times a_7 + 8 \times a_8 + 9 \times a_9$ puis on calcule le reste de la division euclidienne de $S$ par 11. Ce reste est la clé.
Il s'agit d'un entier compris entre 0 et 10 inclus ; s'il vaut 10 on l'écrit alors avec le chiffre romain X.
**1)** Complétez les codes susivants par leur clé :
ISBN 9973 - 719 - 55 - 7.
ISBN 2 - 7427 - 0008.
ISBN 0 - 691 - 05729.
**2)** Un bibliothécaire saisit le code ISBN 2 - 70 - 031999 - 7.Le logiciel lui indique alors qu'il a commis une erreur.
**(a)** Comment le logiciel a-t-il détecté l'erreur?
**(b)**Le bibliothécaire s'aperçoit alors qu'il a interverti les deux chiffres du numéro de l'éditeur ; il saisit donc le code ISBN 2 - 07 - 031999 - 7. Ce code est-il cohérent avec la clé de contrôle ?
**3)** Le bibliothécaire reçoit un nouveau message d'erreur en rentrant le code ISBN 2 - 85368 - 313 - 2. Corriger son erreur, sachant qu'elle porte seulement sur le chiffre de gauche.

**4)** Décrire en langage naturel l'algorithme (le programme) qui permet de détecter éventuelles erreurs de saisie grâce à la clé de contrôle.
**5)** Les propositions suivantes sont-elles justes ou bien fausses ? (justifier rapidement) :
**(a)** « Si la somme *S* est un multiple de 11, alors la clé est 0. »
**(b)** «Si la somme S est un multiple de 10, alors la clé est *X*.»
**(c)** «Toutes les erreurs de saisie sont détectables.»
**(d)** « Si deux codes possèdent la même clé. alors les sommes *S* correspondantes sont congrues modulo 11.»
**6)** Ecrire la réciproque de la dernière proposition puis préciser si cette dernière est juste ou fausse.
**7)** On voudrait savoir si intervertir deux chiffres entraine toujours une modification de la clé, ce qui permet de déceler l'erreur.
On suppose par exemple qu'au lieu de saisir les neuf chiffres d'un code ISBN $a_1a_2a_3a_4a_5a_6a_7a_8a_9$, le bibliothécaire saisisse $a_1a_3a_2a_4a_5a_6a_7a_8a_9$ . On considère les sommes *S* et *S'* correspondant respectivement au code correct et erroné.
**(a)** Calculer *S* - *S'* en fonction des chiffres $a_2$ et $a_3$.
**(b)** Quelles sont les valeurs possibles pour *S* - *S'* ?
**(c)** Est-ce que *S* et S' peuvent être congrues modulo 11 ?
**(d)** Que peut-on en conclure ?

**36** Dans cet exercice, on pourra utiliser le résultat suivant : «Etant donnés deux entiers naturels *a* et *b* non nuls, si PGCD(*a* ; *b*) = 1 alors $PGCD(a^2;b^2)=1$».
Une suite $(S_n)$ est définie pour $n>0$ par $S_n=\sum_{p=1}^{n} p^3$. On se propose de calculer, pour tout entier naturel non nul *n*, le plus grand commun diviseur de $S_n$ et $S_{n+1}$.
**1)** Démontrer que pour tout $n>0$, on a

$$S_n=\left(\frac{n(n+1)}{2}\right)^2 .$$

**2)** Etude de cas où *n* est pair. Soit *k* l'entier naturel non nul tel que $n=2k$.
**a)** démontrer que

$$PGCD(S_{2k};S_{2k+1})=(2k+1)^2\,PGCD(k^2;(k+1)^2)$$

**b)** calculer $PGCD(k;k+1)$ ;

**c)** calculer $PGCD(S_{2k};S_{2k+1})$ .
**3)**Etude de cas où *n* est impair. Soit *k* l'entier naturel non nul tel que $n=2k+1$.
**a)** Démontrer que les entiers $2k+1$ et $2k+3$ sont premiers entre eux.
b) calculer $PGCD(S_{2k+1};S_{2k+2})$.
**4)** Déduire des questions précédentes qu'il existe une unique valeur de *n*, que l'on déterminera, pour laquelle $S_n$ et $S_{n+1}$ sont premiers entre eux.

**La liste des nombres premiers inférieurs à 1000** (sa consultation ne peut que faciliter la résolution de certains exercices). 2-3-5-11-13-17-19-23-29-31-37-41-43-47-53-59-61-67-71-73-79-83-89-97-101-103-107-109-113-127-131-137-139-149-151-157-163-167-173-179-181-191-193-197-199-211-223-227-229-233-239-241-251-257-263-269-271-277-281-283-293-307-311-313-317-331-337-347-349-353-359-367-373-379-383-389-397-401-409-419-421-431-433-439-443-449-457-461-463-467-479-487-491-499-503-509-521-523-541-547-557-563-569-571-577-587-593-599-601-607-613-617-619-631-641-643-647-653-659-661-673-677-683-691-701-709-719-727-733-739-743-751-757-761-769-773-787-797-809-811-821-823-827-829-839-853-857-859-863-877-881-883-887- 907-911-919-929-937-941-947-953-967-971-977-983-991-997.

**Ibn al-Haytham et le théoréme de Wilson**

En 1770, E.WARING enregistrait en deux phrases l'acte de naissance du théorème de Wilson :

"Sit n numerus primus, & $\frac{1.2.3.4...(n-2)(n-1)+1}{3}$ erit integer numerus, e.g. $\frac{1.2+1}{3}=1$,

$\frac{1.2.3.4+1}{5}=5, \frac{1.2.3.4.5.6+1}{7}=103$ &c.Hanc maxime elegantem primorum numerorum pro

prietatem invenit vir clarissimus, rerumque mathematicorum peritissimus Joannes Wilson Armiger ".

Bien que ce théorème n'ait cessé depuis d'être attribué à J.Wilson, à aucun moment E.Waring ne laisse entendre que celui-ci en a donné la démonstration ; et, du reste, tout concourt à montrer que Wilson ne détenait pas la démonstration du théorème qui porte son nom. Aussi WARING, après avoir cité ce théorème et quelques autres qui s'y rapportent, écrit-il:

3Demonstrationes vero hujjusmodi propositionum eo magis difficiles erunt, quod nulla fingi potesi notatio, quae primum numerum exprimit"

C'est seulement grâce à une meilleur connaissance des manuscrits de LEIBNIZ que se trouve ébranlé e la priorité de WILSON, unanimement admise jusque là par les historiens. A la fin du siècle dernier, en effet, G.VACCA a pu trouver chez LEIBNIZ une formulation équivalente de ce même théorème, et bien antérieure par conséquent à celle de WILSON. Et de fait le texte de LEIBNIZ ne permet aucun doute: "Productus continuorum usque ad numerum qui antepraecedit datum divisus per datum relinquit 1, si datus sit primitivus. Si datus sit derivativus, relinquet numerum qui cum dato habeat communem mensuram unitate majorem".

On peut ainsi traduire la proposition de LEIBNIZ:

Si p est un nombre premier, alors $(p-2)! \equiv 1 \pmod{p}$

Il fallut attendre 1771 pour que fut démontré ce théorème.

C'est LAGRANGE qui en donna la démonstration,
de deux manières; la première est directe; la deuxième
consiste à déduire le théorème de WILSON du petit théorème
de FERMAT. LAGRANGE montre en outre la réciproque
de l'énoncé de WILSON, si bien que l'on aboutit finalement au théorème suivant:


Si n > 1, les deux conditions suivantes sont équivalentes:

a) $n$ est premier

b) $(n-1)! \equiv -1 \pmod{n}$

Ainsi se présente l'histoire connue du théorème de WILSON. Or, bien avant LEIBNIZ, un mathématicien du X éme siécle avait énoncé ce même théorème, en des termes aussi précis que ceux que rapporte WARING. Nous allons en effet montrer que dans un Opuscule dont on trouve ici même l'édition et la traduction, le célèbre mathématicien et physicien IBN AL-HAYTHEM (965-1040) présente au cours de sa solution d'un problème de congruences linéaires le théorème de WILSON comme une proposition exprimant précisément "une propriété nécessaire" des nombres premiers, autrement dit une propriété appartenant à ceux-ci "exclusivement".

Il est de bonne méthode de commencer par suivre l'ordre d'exposition d'IBN AL- HAYTHAM lui-même, pour voir comment il situe le dit théorème dans sa propre étude, et pour saisir quelle fonction il lui assigne.

IBN AL-HAYTHAM propose dans cet Opuscule de résoudre le système $(1)\begin{cases} x \equiv 1 \pmod{m_i} \\ x \equiv 0 \pmod{p} \end{cases}$

avec p un nombre premier, et $1 < m_i \leq p - 1$. Nous sommes donc en présence d'un cas particulier du célèbre théorème chinois ,aprés avoir affirmé qu'il s'agit d'un problème qui admet une infinité de solutions entières,....

Recherches sur l'histoire des mathématiques arabes ( R. RAHED)