Mathématiques discrètes

Partie 1 : arithmétique

Résumé de cours, exemples corrigés et exercices

BUT INFORMATIQUE
Semestre 1
R1.06

Marie Deletombe
Moulay-Driss Benchiboun

Cours moodle : R 1.06 : Mathématiques Discrètes
Clé d'inscription : eehq92

marie.deletombe@univ-lille.fr

version du 16 août 2025

Leçon 1 : La division euclidienne

1. Objectifs

Il s'agit de :

- bien comprendre la définition d'une division euclidienne.
- reconnaitre des situations où interviennent des divisions euclidiennes.

2. Un peu de cours

Définition 1

Soient a et b deux entiers relatifs.

3. Pratique guidée - Exercices corrigés

Exemple 1 : Comment effectuer une division euclidienne avec la calculatrice

Faire la division euclidienne de 1789 par 110.

Exemple 2 : lorsque a est négatif

Effectuer la division euclidienne de $a = -40$ par $b = 15$.

4. Les exercices

4.1. Les exercices de base

❒ **Exercice 1 : Quelques divisions euclidiennes**
Indiquer les résultats (quotient et reste) des divisions euclidiennes suivantes :

1. a) 700 par 294.
   b) 294 par 700.
   c) 294000 par 700.
2. a) -700 par 294.
   b) 700 par -294.
   c) -700 par -294.

❒ **Exercice 2 :**
Sachant que $36202744 = 9658 \times 3748 + 4560$, donner le quotient de la division euclidienne de 36202744 par 3748.

❒ **Exercice 3 :**
Vous comptez de 7 en 7, à partir de 38, jusqu'au plus grand nombre inférieur ou égal à 365.

1. Quel est le dernier nombre atteint ?
2. Combien y a-t-il de nombres atteints (38 y compris) ?
3. Par quels nombres peut-on remplacer 365 sans modifier les deux réponses précédentes ?

❒ **Exercice 4 : Calendrier**

1. Quelle heure sera-t-il dans 42h ? dans 1764h ?
2. Quel sera le jour de la semaine dans 42 jours ? dans 1764 jours ?

❒ **Exercice 5 : Le typographe fou**
Un typographe décide de composer un texte de 13579 caractères, constitué de la juxtaposition des 26 lettres de l'alphabet latin abc....xyz répétées aussi longtemps que nécessaire.
Chaque ligne compte 80 caractères, chaque page comporte 34 lignes.

1. Quelle est la première ligne de ce livre ?
2. Donner le nombre de lignes, et le nombre de pages.
3. Quelle est la dernière ligne de ce livre ?

❒ **Exercice 6 : Trouver le nombre**
Lorsqu'un nombre est divisé par 69, le reste est 35. Le même nombre divisé cette fois par 75, a le même quotient mais a cette fois pour reste 17.
Quel est ce nombre ?

4.2. Pour s'entrainer

❒ **Exercice 7 : divisions euclidiennes avec des négatifs**
Indiquer le quotient et le reste des divisions euclidiennes suivantes :

1. 1515 par 456
2. -1515 par -456
3. 456 par 1515

❒ **Exercice 8 :**
Les divisions euclidiennes d'un entier naturel par 155 et par 161 donnent le même quotient et des restes respectivement égaux à 65 et 23.
Déterminer cet entier.

❒ **Exercice 9 :**
Le premier janvier 2000 était un samedi. Quel jour de la semaine était le 275-ème jour de l'année 2000 ?

❒ **Exercice 10 :**
Le compas d'un bateau à la dérive tourne de 7° dans le sens horaire toutes les 8 minutes.
Quelle direction indique le compas après 3 jours, 2 heures et 32 minutes si la direction initiale était de 23° ?

4.3. Pour aller plus loin

❒ **Exercice 11 : quand les quotients sont différents**
Une machine emballe des pièces (toutes identiques) dans des sacs (tous identiques). Le nombre de pièces par sac est constant. Quand la machine emballe 7912 pièces, il reste 37 pièces. Quand elle emballe 59167 pièces, il reste 42 pièces.
Combien y a-t-il de pièces dans chaque sac ?

❒ **Exercice 12 : calcul littéral**
soient $a \geqslant 0$ et $b > 0$ deux entiers.
On note q et r le quotient et le reste dans la division euclidienne de a par b.
Quels sont le quotient et le reste dans la division de $-a$ par b ? de a par $-b$? de $-a$ par $-b$?

Leçon 2 : Les bases

1. Objectifs

Il s'agit de :

- savoir lire et écrire un entier (positif) dans n'importe quelle base b.
- savoir passer d'une base à une autre
- savoir faire des additions et multiplications en base 2.

Afin de mieux comprendre la notion de base, nous mettrons en œuvre des bases *exotiques* (trois, neuf, ...) que vous ne verrez pas en informatique réel.

2. Un peu de cours

Lorsque la base n'est pas précisée, c'est que l'on travaille en base 10 (celle utilisée lorsque l'on apprend à compter).
Lorsque l'on écrit 32645, qu'est-ce que cela signifie fondamentalement ?

Définition 2

De manière générale, en base b, on a :

3. Pratique guidée - Exercices corrigés

Exemple 3 : Convertir en base 10

On passe par la définition, et donc par les puissances de la base.

$(1789)_{10} =$

$(1789)_{16} =$

$(1789)_{8}=$

Remarque 1

En base 16, on écrit $10 = a, \quad 11 = b, \quad 12 = c, \quad 13 = d, \quad 14 = e, \quad 15 = f$

Exemple 4 : Comment écrire un nombre en base b

1. **Écrire 1789 en base 16 (passer de la base 10 à la base 16)**
   1re méthode : succession de divisions euclidiennes.

   2e méthode : recherche des puissances de la base

   .

2. **Écrire 1789 en base 2 (passer de la base 16 à la base 2)**
   Comme $16 = 2^4$, chaque bit de la base 16 peut s'écrire avec 4 bit de la base 2.

3. **Écrire 1789 en base 16 (passer de la base 2 à la base 16)**

4. Les exercices

4.1. Les exercices de base

❒ **Exercice 13 :**

On considère un nombre N écrit en base 10. Déterminer N sachant que

1. le chiffre des unités de N est 3
2. le nombre de centaines de N est 247
3. le chiffre des dizaines de N est 2

❒ **Exercice 14 :**

1. Ecrire en base 10 le nombre $(10101111111)_2$.
2. Ecrire en base 10 le nombre $(2ae0b)_{16}$.
3. Ecrire en base 2 le nombre $(3146)_8$.
4. Ecrire en base 8 l'entier $(abba)_{16}$.

❒ **Exercice 15 :** **Conversion entre bases**

1. Écrire en base 10 les nombres suivants : $(23)_4$, $(10)_5$,$(1000)_2$,$(143)_7$.
2. Déterminer l'écriture du nombre 12345 en base 7, en base 11 et en base 20.
3. Écrire en base 2, 3, 5, 9, 10, 16 les nombres trois, cinq, dix, onze, treize, vingt-huit, huit-cent-quarante-cinq.

❒ **Exercice 16 :** **Vrai ou faux**

Dire si les affirmations sont vraies ou fausses et justifier.

- $(4567)_{16}$ est le nombre $4\times1600+5\times160+5\times16+7$
- $(110110)_2$ est le nombre $1\times2^6+1\times2^5+1\times2^3+1\times2^2$
- $(2345)_5$ est le nombre 350

❒ **Exercice 17 :** **Arithmétique binaire**

1. Calculer "à la main", c'est-à-dire en posant les opérations, les nombres $1789+1515$ et 1789×1515
2. Calculer de manière analogue (en calculant en binaire et sans utiliser la base 10) la somme et le produit des entiers $(1110)_2$ et $(1011)_2$.
   Écrire au préalable les tables de multiplication en base 2.

❒ **Exercice 18 :** **Dans quelle(s) base(s) b peut-on écrire que ...**

1. $(32)_b\times(14)_b=(438)_b$
2. $(27)_b\times(35)_b=(758)_b$
3. $(23)_b\times(34)_b=(910)_b$
4. $(123)_b+(234)_b=(357)_b$

4.2. Pour s'entrainer

❒ **Exercice 19 : Conversions**

Écrire en base 2, 3, 5, 7, 8, 9, 10, 16 les nombres quatre, six, douze, quinze, trente-trois, cent-vingt-huit.

❒ **Exercice 20 : Arithmétique binaire**

Effectuer les calculs suivants en posant l'opération et sans utiliser la base 10 :

1. $(101)_2 + (100011)_2$.
2. $(10010)_2 + (101)_2$.
3. $(1011)_2 \times (1001)_2$.

4.3. Pour aller plus loin

❒ **Exercice 21 :**

Déterminer les nombres à 3 chiffres en écriture décimale qui vérifient les trois conditions suivantes :

1. ce n'est pas un multiple de 10
2. le chiffre des dizaines est quadruple de celui des unités
3. en retranchant 297 à ce nombre, on obtient le nombre écrit à l'envers (par exemple, si le nombre de départ est 721, on obtient 127).

Leçon 3 : Arithmétique

1. Objectifs

Il s'agit de :

- revoir (ou voir) la notion de nombres premiers
- savoir décomposer un nombre en produit de facteurs premiers.
- savoir trouver le nombre et la liste des diviseurs d'un entier.
- revoir (ou voir) plusieurs méthodes pour le calcul du PGCD et du PPCM de deux entiers.

2. Un peu de cours

2.1. Rappel sur le calcul de puissances

$(a \times b)^m =$

$a^{m+n} =$

$(a^m)^n =$

2.2. Nombres premiers et décomposition

Définition 3 : diviseur, multiple

On dira que :

- b ***divise*** a
- a est un ***multiple*** de b
- b est un ***diviseur*** de a

si

Propriété 1

Soient a et b des entiers, b étant non nul.
Le nombre b divise a si et seulement si .

Exemple 5

5 divise 15 car il existe $k \in \mathbb{Z}$ tel que

Définition 4 : nombre premier

Un entier $p > 1$ est dit ***premier*** lorsqu'il a exactement deux diviseurs : 1 et lui-même.

Propriété 2 : décomposition en produit de facteurs premiers

Tout entier a peut être décomposé en produit de nombres premiers, et cette décomposition est unique.

Les p_i sont des nombres premiers distincts.
Les exposants α_i sont des entiers naturels non nuls.

2.3. PGCD, PPCM

Définition 5 : PGCD, PPCM

- ***PGCD***(a, b)=
  On le note aussi .
- ***PPCM***(a, b)=
  On le note aussi .

Propriété 3 : caractérisation du PGCD

Définition 6 : premiers entre eux

On dit que deux entiers a et b sont ***premiers entre eux*** si .

Théorème 1 : théorème de Bezout

3. Pratique guidée - Exercices corrigés

Exemple 6 : Décomposer un entier en produit de facteurs premiers

Donner la décomposition en facteurs premiers de 132 et 108.

Exemple 7 : Liste des diviseurs d'un entier

Donner la liste des diviseurs de 132.

Exemple 8 : Calcul du PGCD et du PPCM par la décomposition

Calculer le PGCD et le PPCM de 132 et 108.

On utilise ensuite les propriétés ci-dessous :

-
-

Exemple 9 : Calcul du PGCD par l'algorithme d'Euclide

Calculer le PGCD et le PPCM de 132 et 108.
On effectue une série de divisions euclidiennes.

Alors, le PGCD est le **dernier reste non nul**.

4. Les exercices

4.1. Les exercices de base

❒ **Exercice 22 : décomposition en produit de facteurs premiers**
Donner la décomposition en produits de facteurs premiers de chacun des entiers suivants : 111, 1025, 6788, 121212, 2020, 2021.

❒ **Exercice 23 : décomposition en produit de facteurs premiers et diviseurs**

1. Donner la décomposition en produits de facteurs premiers de chacun des entiers suivants : 1500, -199, $6!$, 105.
2. Pour chacun de ces entiers, donner la liste de ses diviseurs.
3. Quels sont les diviseurs communs à 1500 et à 105 ? Quel est le plus grand d'entre eux ?

❒ **Exercice 24 : décomposition en produit de facteurs premiers et PGCD**
Soient les entiers $a = 1040400$ et $b = 39000$.

1. Donner la décompostion en produit de facteurs premiers de a et b.
2. En déduire la valeur de $a \wedge b$.
3. Retrouver la valeur de $a \wedge b$ par l'algorithme d'Euclide.
4. Que valent les PGCD suivants : $a \wedge b^2$, $169a \wedge b^2$, $a \wedge b \wedge 340$?

❒ **Exercice 25 : décomposition en produit de facteurs premiers et PGCD/PPCM**
Soient $a = 7392$ et $b = 1400$

1. Donner la décompostion en produit de facteurs premiers de a et b.
2. En déduire leur PGCD et leur PPCM.
3. Comparer les produits $(a \wedge b)(a \vee b)$ et ab.
4. Déterminer les entiers a' et b' tels que $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$.
   Que peut-on dire de $a' \wedge b'$?

❒ **Exercice 26 : décomposition en produit de facteurs premiers**

1. Est-il possible de trouver deux entiers a et b tels que : $a \wedge b = 50$ et $a \times b = 220000$?
   Si non, expiquer pourquoi ; si oui, donner toutes les solutions du problème.
2. Même question pour $a \wedge b = 200$ et $a \times b = 220000$

4.2. Pour s'entrainer

❒ **Exercice 27 : décomposition en produit de facteurs premiers**
Donner la décomposition en produits de facteurs premiers de chacun des entiers suivants : 231, 153, 600, 221, 211.

❒ **Exercice 28 : nombre de diviseurs**
Quel est le nombre de diviseurs des nombres suivants : 20, 48, 180 ?

❒ **Exercice 29 : Calcul de PGCD et PPCM**
Donner le PGCD et le PPCM des couples d'entiers suivants : 8 et 42 ; 24 et 15 ; 49 et 14 ; 22 et 48.
Pour le calcul du PGCD, on pourra utiliser les deux méthodes (décomposition, Euclide)

4.3. Pour aller plus loin

❒ **Exercice 30 :**

Le PGCD de deux nombres est 18. Leur PPCM est 648.
Quels sont ces deux nombres ?.

❒ **Exercice 31 :**

1. Deux nombres a et b sont premiers entre eux et leur somme est 24.
   Déterminer tous les couples (a,b) possibles.
2. Déterminer tous les couples $(x;y)$ d'entiers naturels tels $x+y=96$ et $PGCD(x;y)=4$.

❒ **Exercice 32 :**

Un entier N a pour écriture décimale $72a83b$.
Déterminer N sachant qu'il est divisible par 6 et par 45.
On pourra commencer par trouver la valeur de b.

Leçon 4 : Calcul modulaire

1. Objectifs

Il s'agit de :

- manipuler des calculs modulaires élémentaires.
- reconnaitre la notion d'inversible.
- résoudre des équations modulaires.
- découvrir la fonction d'Euler.

2. Un peu de cours

2.1. Congruences modulo m

Définition 7 : congruence modulo m

Soient a, b et m des entiers relatifs tels que $m \neq 0$.

$$\begin{aligned} a \equiv b \ [m] &\iff \\ &\iff \\ &\iff \\ &\iff \end{aligned}$$

On dit que ***a est congru à b modulo m***.

Exemple 10

$17 \equiv 2 \ [5]$ car
$17 \equiv 2 \ [5]$ car
$17 \equiv 2 \ [5]$ car
$17 \equiv 2 \ [5]$ car

Propriété 4

Soient x et m des entiers relatifs tels que $m \geqslant 2$.
Il existe un unique $\alpha \in [\![0 \ ; \ m-1]\!]$ tel que $x \equiv \alpha \ [m]$

Exemple 11

$17 \equiv \mathbf{2} \ [5]$
Mais on a aussi $17 \equiv 7 \ [5]$ et $17 \equiv 37 \ [5]$ et $17 \equiv -3 \ [5]$ (une infinité de possibilités).
Mais 2 est l'unique entier dans l'intervalle $[\![0 \ ; \ 4]\!]$.

Définition 8 : classe d'équivalence modulo m

L'ensemble $\{y \in \mathbb{Z} / y \equiv x \ [m]\}$ est appelé ***la classe d'équivalence de x modulo m***.
On la note $[x]_m$.

Exemple 12

$[17]_5 = \{ \qquad \qquad \qquad \qquad \}$

Définition 9 : $\mathbb{Z}/m\mathbb{Z}$

On note $\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, [2]_m, ..., [m-1]_m\}$

Remarque 2

Par souci de simplification, nous écrirons $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, ..., m-1\}$

Propriété 5 : règles de calculs

Soient a, a', b, b' et m des entiers tels que $m \neq 0$.
Si $a \equiv a' \ [m]$ et $b \equiv b' \ [m]$,
Alors :

-
-
-

2.2. Inversibilité

Définition 10 : inverse modulo m

Soient a, b et m des entiers tels que $m \geqslant 2$.
On dit que b ***est l'inverse de*** a ***modulo*** m ***si*** [a]

[a]. Cette égalité permet également de dire que a ***est l'inverse de*** b ***modulo*** m.

Exemple 13

$13 \times 7 \equiv 1 \ [15]$ (car $13 \times 7 = 1 + 6 \times 15$), donc 7 est l'inverse de 13 modulo 15.
Mais cela nous indique aussi que

Théorème 2 : rappel du chapitre précédent - théorème de Bezout

En particulier si $d = 1$, on a :

Exemple 14

Si l'on reprend l'exemple 13, on a : $13 \times 7 - 6 \times 15 = 1 \leftarrow$ c'est l'**égalité de Bezout**.
L'égalité de Bezout va donc nous permettre de trouver des inverses modulaires.

Propriété 6 : Critère d'inversibilité

Soient a, b et m des entiers tels que $m \geqslant 2$.
a est ***inversible*** modulo m si et seulement si

2.3. Fonction d'Euler

Définition 11 : fonction Φ d'Euler

Soient m un entier strictement positif.
On note $\Phi(m)$.

Exemple 15

$\mathbb{Z}/16\mathbb{Z} =$
Les éléments inversibles sont ceux qui sont
Donc $\mathbb{Z}/16\mathbb{Z}^* =$
Et $\Phi(16) =$.

Propriété 7 : calcul de $\Phi(m)$

-
-
-

Exemple 16

$\Phi(15) =$
$\Phi(16) =$

Théorème 3 : théorème d'Euler

Si $x \wedge m = 1$, alors

Exemple 17

$2 \wedge 15 = 1$, donc

3. Pratique guidée - Exercices corrigés

Exemple 18 : Trouver l'inverse d'un nombre

Trouver l'inverse de 11 modulo 9.
$11 \wedge 9 = 1$, donc 11 est inversible modulo 9.

1re méthode : algorithme d'Euclide inversé.
On commence par dérouler l'algorithme d'Euclide :

On isole le reste "1" de la deuxième ligne :
On isole le reste "2" de la première ligne :

On aboutit à l'identité de Bezout :
Que l'on peut réécrire :
Autrement dit, par définition de la congruence,

2e méthode : algorithme de XGCD
Chaque étape de cet algorithme aboutit à un triplet (d, u, v) qui vérifie : $d = 11u + 9v$

t_a	t_b	div eucl	t_r

Le triplet $(1, -4, 5)$, nous donne la relation :

Exemple 19 : Résoudre une équation modulaire

Résoudre l'équation $11x \equiv 7\ [9]$.

Exemple 20 : Calculer $\Phi(m)$

Calculer $\Phi(45)$.

Exemple 21 : Puissance modulaire

- Calculer $2^{24}\ [45]$
- Calculer $2^{78}\ [45]$
  L'idée ici est d'utiliser le théorème d'Euler pour faire baisser la puissance.

4. Les exercices

4.1. Les exercices de base

❒ Exercice 33 : compréhension de la définition

1. Déterminer a entier compris entre 0 et 5 tel que : $802 \equiv a$ [6]
2. Déterminer a entier compris entre 0 et 8 tel que : $304 \equiv a$ [9]
3. Parmi les affirmations suivantes, décider celles qui sont vraies et celles qui sont fausses :
   $115 \equiv 27\ [11]$ $\quad 115 \equiv 27\ [-11]$ $\quad -39 \equiv 27\ [11]$ $\quad 39 \equiv 27\ [11]$ $\quad -39 \equiv -27\ [11]$
4. Trouver les entiers n compris entre 0 et 100 qui vérifient à la fois $n \equiv 27$ [11] et $n \equiv 4$ [7]
5. Combien y a-t-il d'entiers compris entre 0 et 1000 qui sont congrus à 17 modulo 89 ? à 89 modulo 17 ?
6. Combien y a-t-il d'entiers compris entre 0 et 1000 qui sont congrus à 17 modulo 90 ? à 18 modulo 100 ? aux deux à la fois ?

❒ Exercice 34 : propriétés et inversibilité

1. Calculer :

$$14\ [89] + 7\ [89] \qquad 14\ [89] \times 7\ [89] \qquad 1788^{1515}\ [1789]$$

2. Construire les tables d'addition et de multiplication de $\mathbb{Z}/5\mathbb{Z}$.
   Quels sont les inversibles de $\mathbb{Z}/5\mathbb{Z}$?

	0	1	2	3	4
0					
1					
2					
3					
4					

	0	1	2	3	4
0					
1					
2					
3					
4					

3. Mêmes questions pour $\mathbb{Z}/6\mathbb{Z}$.

	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

4. Mêmes questions pour $\mathbb{Z}/2\mathbb{Z}$. Comment nomme-t-on ces opérations dans le cours d'architecture ?

	0	1
0		
1		

	0	1
0		
1		

❒ Exercice 35 : Calcul d'inverse modulo n

1. Les nombres 3, 6 et 15 sont-ils inversibles modulo 16 ? Si oui, donner leur inverse modulo 16 ? (on donnera l'entier compris entre 0 et 15).

2. 13 est-il inversible modulo 100 ? Si oui, déterminer son inverse en utilisant les deux méthodes possibles (Euclide inversé et XGCD)

❒ **Exercice 36 : équations modulaires**

1. Par un calcul direct, montrer que 19 et 73 sont inverses modulo 99.
2. 99 est-il inversible modulo 19 ? Si oui, déterminer son inverse en utilisant deux méthodes possibles (Euclide inversé et XGCD)
3. Résoudre les équations et systèmes d'équations suivants (les inconnues sont des entiers) :

$$19x \equiv 76 \; [99] \qquad 99x \equiv 2004 \; [19] \qquad \begin{cases} 10x+7y=76 \; [99] \\ 3x+4y=45 \; [99] \end{cases}$$

❒ **Exercice 37 : fonction d'Euler**

A partir de leur décomposition en produit des facteurs premiers (cf. exercice 1), donner la valeur de $\Phi(n)$ pour les nombres entiers n suivants :

$$111, \quad 1025, \quad 6788, \quad 121212, \quad 2020, \quad 2021$$

❒ **Exercice 38 : calcul de puissances modulaires**

A l'aide du théorème d'Euler, calculer :

1. $123^{45}[100]$
2. $123^{255}[100]$
3. $2003^{427}[1000]$

4.2. Pour s'entrainer

❒ **Exercice 39 :**

1. Trouver un entier n tel que $n \equiv 3 \; [7]$ et $n \equiv 2 \; [9]$
2. Combien y a-t-il d'entiers compris entre 0 et 1000 qui sont congrus à 12 modulo 67 ? à 67 modulo 12 ?

❒ **Exercice 40 : d'autres équations pour s'entraîner**

1. 17 est-il inversible modulo 100 ? Si oui, déterminer son inverse par XGCD.
2. Résoudre les équations et systèmes d'équations suivants (les inconnues sont des entiers) :

$$17x \equiv 68 \; [100] \qquad 17x \equiv 2 \; [100] \qquad 100x \equiv 58 \; [17] \qquad 100x \equiv 17 \; [58] \qquad \begin{cases} x+2y=95 \; [100] \\ 3x+23y=98 \; [100] \end{cases}$$

❒ **Exercice 41 : calcul de puissances modulaires**

A l'aide du théorème d'Euler, calculer :

1. $133^{47}[100]$
2. $1903^{413}[1000]$

4.3. Pour aller plus loin

❒ **Exercice 42 : Critères de divisibilité**

Rappeler et démontrer les critères de divisibilité d'un nombre entier par 2, 5, 9, 3, 4, 11.