S5 : 2020-2021

Nathan TONNELLE

MINF0501

Arithmétique

Table des matières

[Plan de cours 3](#_Toc52373519)

[Chapitre 1 : Divisibilité dans 3](#_Toc52373520)

[Définition 3](#_Toc52373521)

[Exemple 3](#_Toc52373522)

[Remarque 3](#_Toc52373523)

[Exemple 3](#_Toc52373524)

[Propriété 3](#_Toc52373525)

[Démonstration 3](#_Toc52373526)

[Exemple 3](#_Toc52373527)

[Propriété 4](#_Toc52373528)

[Démonstration 4](#_Toc52373529)

[Définition 4](#_Toc52373530)

[Propriété 4](#_Toc52373531)

[Remarque 4](#_Toc52373532)

[Exemple 4](#_Toc52373533)

[Division Euclidienne 5](#_Toc52373534)

[Propriété – définition 5](#_Toc52373535)

[Schéma 5](#_Toc52373536)

[Exemple 5](#_Toc52373537)

[Propriété 5](#_Toc52373538)

[Exemple 5](#_Toc52373539)

[Remarque 5](#_Toc52373540)

[Application 5](#_Toc52373541)

[Définition 5](#_Toc52373542)

[Exemple 5](#_Toc52373543)

[Méthode 6](#_Toc52373544)

[Notions de PGCD et algorithme d'Euclide 7](#_Toc52373545)

[Définition 7](#_Toc52373546)

[Remarque 7](#_Toc52373547)

[Exemple 7](#_Toc52373548)

[Propriété 7](#_Toc52373549)

[Démonstration 7](#_Toc52373550)

[Exemple 7](#_Toc52373551)

[Méthode 7](#_Toc52373552)

[Exemple 8](#_Toc52373553)

[Propriété 8](#_Toc52373554)

[Définition 8](#_Toc52373555)

[Exemple 8](#_Toc52373556)

[Propriété 8](#_Toc52373557)

[Exemple 8](#_Toc52373558)

[Théorème de Bézout, Gauss 9](#_Toc52373559)

[Propriété (égalité de Bézout) : 9](#_Toc52373560)

[Exemple 9](#_Toc52373561)

[Théorème de Bézout 9](#_Toc52373562)

[Démonstration 9](#_Toc52373563)

[Exemple 9](#_Toc52373564)

[Théorème de Gauss 9](#_Toc52373565)

[Exercice 9](#_Toc52373566)

[Corollaire 10](#_Toc52373567)

[Démo 10](#_Toc52373568)

[Application 10](#_Toc52373569)

[Application : les équations diophantiennes 10](#_Toc52373570)

[Définition 10](#_Toc52373571)

[Exemple 10](#_Toc52373572)

[Propriété 10](#_Toc52373573)

[Exemple 10](#_Toc52373574)

[Méthode 10](#_Toc52373575)

[1er étape 10](#_Toc52373576)

[2ème étape 10](#_Toc52373577)

[PPCM et lien avec PGCD 12](#_Toc52373578)

[Définition 12](#_Toc52373579)

[Exemple 12](#_Toc52373580)

[Propriété 12](#_Toc52373581)

[Propriété 12](#_Toc52373582)

[Exercice 12](#_Toc52373583)

[Chapitre 2 : nombres premiers 13](#_Toc52373584)

[Définition 13](#_Toc52373585)

[Exemple 13](#_Toc52373586)

# Plan de cours

Divisibilité dans

Nombres premiers

Relation de congruence et /n

Arithmétique sur K[x] où K est un corps

# Chapitre 1 : Divisibilité dans

On rappelle que ={0; 1; 2; …}

={…; -2; -1; 0; 1; 2; …}

Dans tout ce coures les nombres considérés sont dans

## Définition

Soient **a**, **b** € . On dit que **b** divise **a** s'il existe **k**€ tel que **a**=**bk**.

Dans ce cas on note **b**/**a** et **b** est appelé un diviseur de **a**, où **a** est un multiple de **b**.

## Exemple

Listons les diviseurs de 30 :

* 1; 2; 3; 5; 6; 10; 15; 30;
* -1; -2; -3; -5; -6; -10; -15; -30

Donnons des multiples de 11 :

* 0; 11; 22; -44; -66; …

## Remarque

Si n€, 1; -1; n; -n sont toujours des diviseurs de

## Exemple

Les billets de 5€ possèdent un numéro de série possédant 1 ou 2 lettres et 11 ou 10 chiffres. On associe à chaque lettre une valeur : A=11; B=12; …; Z=36. On crée alors un nombre à 13 ou 14 chiffres. Ce nombre est divisible par 9.

## Propriété

Soient a, b, c €

1. b/a ⬄ b/-a ⬄ -b/a ⬄ -b/-b
2. si c/a et c/b alors c/na+mb où (n,m) €
3. si c/b et b/a alors c/a

## Démonstration

c/a ⬄ , a = ck

c/b ⬄ , b = ck'

na +mb = nck+mck'

= c(nk+mk')

nk+mk' car n; m; k; k' ( et est un anneau)

Donc c/na+mb

3) c/b ⬄ , b=ck

b/a ⬄ , a=bk'

Ainsi a=bk' a=(ck)k' a=ckk'

kk'

Donc c/a

## Exemple

1. Déterminer les n tels que n-4 est divisible par 7

7/n-4 ⬄ , n-4 = 7k

⬄ ; n=7k+4

1. Soit , montrer que si **d** divise et **d** divise alors d/4

{d/6k+1

{d/10k+3

Donc **d** divise toute combinaison linéaire de +k+1 et 10k+3

Ainsi d/**5**(6k+1)-**3**(10k+3)

d/-4 ⬄ d/4

## Propriété

Soient **a**, **b**

1. Si a ≠0 et b/a alors |b| ≤|a|
2. Si b/a et a/b alors a=±b

Dans ce cas, **a** et **b** sont dits associés

## Démonstration

b/a , a=bk

a≠0 ⬄ k≠0 donc |k| ≥1

|a| = |bk| = |b|\*|k|

≥|b|

## Définition

Soit a .

On note D(a), l'ensemble des diviseurs de a.

## Propriété

Si a D(a) est fini

## Remarque

D(0)=

## Exemple

Déterminer les entiers naturels vérifiant

Déterminons D(16)

D(16) ={1; 2; 4; 8; 16; -16; -8; -4; -2; -1}

Il y a plusieurs cas :

* et ⬄ {x=5; y=16}
* et ⬄ {x=6; y=8}
* et ⬄ {x=8; y=4}
* ⬄ {x=12; y=2}
* ⬄ {x=20 ; y=1}
* ⬄ {x=3; y=-16}

On n'étudie pas la suite des cas car ici y < 0

Les solutions sont :

S = {(5;16); (6;8); (8;4); (12;2); (20;1)}

# Division Euclidienne

## Propriété – définition

Soient ,

Il existe un unique couple (q,r) tel que

Effectuer la division euclidienne de **a** par **b**, c'est trouver ces nombres **q** et **r** (quotient et reste)

## Schéma

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 0 | |  | b | |  | 2b | |  | 3b | |  | … | |  | qb | |  | a=bq+r | |  | (q+1)b | |  |  |
|  | | |  | | |  | | |  | | |  | | |  | | | [ | | |  | | | [ | | |
|  | | |  | | |  | | |  | | |  | | |  | | | [ | | |  | | | [ | | |

## Exemple

Déterminer la DE (division Euclidienne) de 4543 par 7

**Schéma 3**

4543=7\*649+0 reste quotient

713=16\*43+25

Donner le quotient et le reste de la DE de :

1. 713 par 16

713=16\*44+9

1. 713 par 43

713=16\*43+25

## Propriété

DE dans .

Soient **a**, **b**

Il existe un unique couple (q,r) tel que : et , q et r sont respectivement le quotient de et le reste de la DE de **a** par **b**.

## Exemple

Ecrire la DE de

Donc q=9 et r=3

## Remarque

1. Si r=0 alors b/a
2. , a=bq ou a=bq+1 … ou a=bq+b-1

## Application

Ecriture d'un entier en base b

Notre système de numération repose sur le nombre 10, ses puissances et sur les 10 chiffres 0; 1; 2; …; 9.

On parle de numération décimale, en base 10.

## Définition

Un entier naturel N en base b s'écrit sous la forme : N=(an,an-1, …,a1,a0)

Avec

Ce nombre s'écrit dans notre système de numération :

## Exemple

A l'inverse, comment écrire 326 en base 2 ?

Nous allons utiliser une suite de division euclidienne par 2

## Méthode

Pour convertir un nombre du système décimal dans une base b, il suffit de diviser successivement ce nombre et ses quotients par b jusqu'à obtenir un quotient nul.

# Notions de PGCD et algorithme d'Euclide

## Définition

Soient a, b, non simultanément nuls.

Le plus grand élément de D(a)D(b) est appelé le plus grand diviseur commun de a et b. on le note PGCD(a;b) ou (\wedge)

## Remarque

Ainsi D(a)ou D(b) est un ensemble fini et dans tous les cas :

est fini. est une partie de , elle admet donc un plus grand élément.

## Exemple

Calculons : PGCD(45,20)

D'où

## Propriété

Soient

1. Si b/a alors
2. Soient tels que a = bq+r alors

## Démonstration

1. Comme (tout diviseur de b divise a car b/a)

Donc et b est le plus grand élément de D(b).

Donc

1. Se déduit de 1) car 1/a et a/0
2. Montrons que

Soit

Déjà

Donc

Ainsi

On peut montrer l'inclusion inverse et voir que

## Exemple

Reprenons le calcul de

**Schéma 4 :**

Posons la division euclidienne de 20 par 5

## Méthode

Algorithme d'Euclide.

Soient . On effectue la division euclidienne de a par b

On effectue maintenant la division de b par r1

On poursuit ainsi jusqu'à obtenir un reste nul.

Le PGCD de a et b est alors égal au dernier reste non nul

## Exemple

Calculer PGCD(2250;612)

A l'aide de l'algorithme d'Euclide, on trouve que le PGCD(2250;612)=18

## Propriété

Soient

|  |  |
| --- | --- |
| {D/a  {D/b | ⬄D/PGCD(a,b) |

Si D est un diviseur commun à a et b alors il divise PGCD(a,b)

## Définition

Soient

On dit que a et b sont premier entre eux si PGCD(a,b)=1.

## Exemple

Montrer que 32 et 15 sont premier entre eux.

PGCD(32;15)

D'après l'algorithme d'Euclide (ils sont premier entre eux)

## Propriété

Soient

Si alors , tels que :

{a=a'd

{b=b'd

{

## Exemple

Déterminer tels que

tels que :

{a=20a'

{b=20b'

{

Les valeurs de a' et b' peuvent être :

0 et 12

1 et 11

2 et 10

3 et 9

4 et 8

5 et 7

6 et 6

Or a' et b' doivent être premiers entre eux

Les valeurs possibles pour a' et b' sont donc :

1 et 11 ou 5 et 7

Ainsi (a;b)=(20;220)=(220;20)=(100;140)=(140;100)

Et ces solutions vérifient

# Théorème de Bézout, Gauss

## Propriété (égalité de Bézout) :

Soient : tels que

Il existe tels que :

## Exemple

Calculer PGCD(156;24)

PGCD(156;24)=12

Ici 156-24\*6=12

Donc u=1 et v=6 convient

PGCD(32;15)=1

Ici on a :

## Théorème de Bézout

Soient a et b sont premiers entre eux,

## Démonstration

Egalité de Bézout avec d=a^b=1

d=a^b

Donc

Et alors

Et alors

Et donc d=1

## Exemple

Soient

D'après le théorème de Bézout

PGCD(3n+2 , 2n+1) = 1 et ce pour tout n entier naturel

## Théorème de Gauss

Soient

Si { alors a|c

{

## Exercice

Déterminer tels que

(\*)

ainsi

Or donc

,

En substituant dans (\*)

S'il y a des solutions, elles s'écrivent (x,y)=(9k , 6+4k) où

Montrons que ces solutions conviennent :

Donc les solutions vérifient

## Corollaire

Si et alors

## Démo

D'après le théorème de Gauss

et

## Application

Pour montrer qu'un nombre est divisible par 6, il suffit de montrer qu'il est divisible par 3 et 2 ()

# Application : les équations diophantiennes

## Définition

Une équation diophantienne est une équation à coefficients entiers et dont on recherche des solutions entières.

## Exemple

## Propriété

Soient

L'équation admet des solutions ssi

## Exemple

Les équations suivantes ont-elles des solutions ?

donc cette équation possède des solutions (entières)

Donc cette équation n'admet pas de solution (entières)

## Méthode

Résolution d'une équation diophantienne

(\*)

### 1er étape

Trouver une solution particulière

(3;1) est une solution particulière.

Si on ne trouve pas de solutions

Appliquer Euclide étendu

### 2ème étape

On a

Or et d'après le théorème de Gauss,

En remplaçant dans (\*) je détermine x

Réciproquement montrons que ces solutions conviennent

Ainsi les solutions sont : avec

# PPCM et lien avec PGCD

## Définition

Soient , le plus petit multiple commun positif à a et b est le plus petit élément des multiples de a et de b.

On le note

## Exemple

15 12

24

30 36

45 46

60 60

75 72

En écrivant les multiples de 12 et 15 on voit que

## Propriété

{M est un multiple de a

{M est un multiple de b

(plus petit au sens de la division)

## Propriété

Soient

En particulier

Si

## Exercice

Déterminer

Idée : calculons

Déterminer les entiers positifs vérifiant :

{

{

{

{

{

sont des diviseurs de 34

Ou

Ou

Ou

# Chapitre 2 : nombres premiers

## Définition

Soit

On dit que p et premier si ses seuls diviseurs positifs sont 1 et p

## Exemple

2; 3; 5; 7; 11; … sont des nombres premiers.

n'est pas premier on dit qu'il est composé

## Remarque

On notera l'ensemble des nombres premiers

2 est le seul nombre premier pair.

## Propriété

Soient

* ou
* alors

## Démonstration

* donc donc

## Application

Montrer que

## Propriété

* admet au moins un diviseur premier
* Si n'admet pas de diviseur premier entre 2 et alors est premier

## Exemple

Montrons que 101

Voyons qui sont les nombres premiers entre 2 et 10 : 2; 3; 5; 7

et alors

## Propriété

L'ensemble des nombres premiers est infini

## Démonstration

Supposons qu'il y en a un nombre fini

On pose

car

D'après la propriété précédente, il existe or , donc or et

Dans ce cas

Et

Ceci est absurde et est infini

## Crible d'Eratosthène

L'idée est d'écrire tous les entiers.

On raye 0 et 1

On garde 2 et on raye ses multiples

On garde les prochains entiers non rayés puis on raye ses multiples et on recommence …

0; 1; 2; 3; 4; 5; 6; 7; 8; 9…

On garde : 2; 3; 5; 7

## Théorème fondamental de l'arithmétique

Tout nombre entier supérieur ou égal à 2 se décompose en produit de facteurs premiers. De plus cette décomposition est unique à l'ordre des facteurs près.

Soient

## Exemple

Décomposer 120 et 354 en produit de nombre premiers

## Utilité

Nombre de diviseurs de 120

**Schéma 5:**

Il y a diviseurs positifs de 120

De même, il y a diviseurs positifs de 354

## Propriété

Soit

possède exactement : diviseurs positifs

Si de plus

s'obtient en multipliant les nombres premiers apparaissant dans les deux décompositions à la puissance la plus petite puissance apparue.

s'obtient en multipliant les nombres premiers avec pour exposant la plus grande puissance apparaissant dans les deux décompositions.

## Exemple

# Congruence et

## 1 : relation de congruence

### Définition

Soient a, b et n

On dit que a et b sont congru modulo n si a et b sont divisible par n.

Dans ce cas on note

### Exemple

### Remarque

Soit

* ssi
* où r est le reste dans la division euclidienne de a par n. r est l'unique entier vérifiant et

### Propriété

Soient

Si alors

### Exemple

**(non)**

La relation de congruence n'est pas compatible avec la division.

### Exercice

Déterminer les entiers n vérifiant

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| N est congrue | 0 | 1 | 2 | 3 | 4 | 5 |
|  | 0 | 3 | 0 | 3 | 0 | 3 |

Il n'existe pas d'entiers tels que

## Théorème : petit théorème de Fermat

Soit , alors pour tout

Si

### Exemple

Calculons :

en effet et 2; 3 et 5 ne divisent pas 41

et comme on a d'après le petit théorème de Fermat

### Système de congruences (théorème des restes chinois)

On cherche n tel que :







* ,

* ,

=> (\*)

Reste à résoudre (\*)

Pour déterminer les valeurs de k et enfin en déduire les valeurs de n.

### Application : Exponentiation modulaire

Comment calculer

#### Méthode naïve

#### Méthode élégante

## 2 : relation d'équivalence

### Définition

Une relation est dite d'équivalence si :

* Elle est réflexive
* Elle est symétrique
* Elle est transitive

### Exemple

La relation " être inférieur à" n'est pas symétrique, ce n'est pas une relation d'équivalence

### Propriété

Soit la relation de congruence modulo n est une relation d'équivalence.

### Définition

On définit la classe d'équivalence d'un entier a comme l'ensemble (classe de a)

On définit alors comme l'ensemble des classes d'équivalences modulo n

et

### Définition

Soit G un ensemble et + une loi de composition

On dit que (G;+) est un groupe si

* + est une loi de composition interne
* + possède un élément neutre
* + est associative
* Tout élément de G possède un symétrique

Si + est commutative alors (G;+) est dit abélien

### Propriété

est un groupe abélien

### Définition

avec A un ensemble et +; x deux lois de composition internes est appelé un anneau si

* (A; +) est un groupe abélien
* x est associative et possède un neutre
* x est distributive sur +

Si x est commutative on parle d'anneau commutatif

### Propriété

est un anneau commutatif

### Exemple

Dans

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \* |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Remarque

* est l'élément neutre de x

### Définition

Un élément est inversible s'il existe tel que

### Exemple

Dans est inversible car

### Propriété

Les éléments inversibles de sont les vérifiant

### Exemple

Les inversibles de sont

### Propriété

Si alors est un corps. C’est-à-dire un anneau dont tous les éléments non nuls sont inversibles pour la loi x

# Arithmétique des polynômes

Ici on appelle

## 1 : division euclidienne PGCD, PPCM

### Définition

Soient

On si que B divise A s'il existe tel que

On note alors

### Exemple

Donc

### Remarque

Les polynômes de degré 0 sont les seuls inversibles de

A est inversible s'il existe B tel que AB=1

### Propriété

Soient

Si A|B et B|A alors A=aB avec et A et B sont dits associés

### Remarque

Dans on aurait

### Théorème

Soient et , il existe un unique couple tel que ( : degré)

### Exemple

DE de par

**Schéma 1 feuille CM 2**

(Quotient \* diviseur + reste)

### Corollaire

Soient et

### Remarque

La division euclidienne existe dans mais aps dans (DE de )

### Définition

Soient

On note

UN polynôme vérifiant

Et si

Alors

### Remarque

Ici le PGCD n'est pas unique. Il l'est si on impose que son coefficient dominant doit être égal à 1.

## 2 : irréductibilité

### Définition

Un polynôme P est dit irréductible si ses seuls diviseurs sont les inversibles et les polynômes qui lui sont associés

### Remarque

Les polynômes irréductibles sont l'équivalent dans des nombres premiers dans

### Propriété

Si P est irréductible et P|A où

Si P divise un produit de polynôme alors P divise l'un d'entre eux.

### Exemple

est irréductible dans

**ATTENTION** et est réductible dans

### Propriété

* Les polynômes de degré 1 sont toujours irréductibles
* Les irréductibles de sont :
  + Les polynômes de degré 1
  + Les polynômes de degré 2 tels que Delta <0
* Les irréductibles de sont exactement les polynômes de degré 1 (d'Alembert Gauss)

### Théorème

Soit

irréductibles

tels que

Tout polynôme se décompose en produit de polynômes irréductibles. Ce produit est unique à l'ordre des facteurs prés.

### Corollaire

Avec les notations précédentes

avec

### Exemple

Alors est un diviseur de P