# Plan de cours

Divisibilité dans

Nombres premiers

Relation de congruence et /n

Arithmétique sur K[x] où K est un corps

# 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

## Démo :

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 alros 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

## Démo :

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 :

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 :