CHAPITRE 1 : Divisibilité - Nombres premiers - Congruences

[1 Divisibilité dans 2](#_Toc428346763)

[1.1 Deux sortes de divisions 2](#_Toc428346764)

[1.2 Diviseurs 3](#_Toc428346765)

[1.3 Nombres premiers entre eux 4](#_Toc428346766)

[1.4 Transitivité de la division 4](#_Toc428346767)

[1.5 Divisibilité de toute combinaison linéaire par tout diviseur commun 5](#_Toc428346768)

[2 La division euclidienne de *a* par *b* 5](#_Toc428346769)

[2.1 Théorème sur l’existence et l’unicité d’un couple d’entiers naturels (*q* ; *r*) 5](#_Toc428346770)

[2.2 Division euclidienne dans 7](#_Toc428346771)

[2.3 Propriétés de la relation de division euclidienne de *a* par *b* 7](#_Toc428346772)

[3 Les nombres premiers 8](#_Toc428346773)

[3.1 Définition d’un nombre premier 8](#_Toc428346774)

[3.2 Théorème des diviseurs premiers 9](#_Toc428346775)

[3.3 Tester la primalité 11](#_Toc428346776)

[3.4 Théorème sur l’infinité des nombres premiers 12](#_Toc428346777)

[4 Existence et unicité de la décomposition en facteurs premiers 13](#_Toc428346778)

[4.1 Théorème fondamental de l’arithmétique 13](#_Toc428346779)

[4.2 Théorème sur la forme des diviseurs 15](#_Toc428346780)

[4.3 Nombre de diviseurs d’un entier naturel supérieur ou égal à 2 16](#_Toc428346781)

[5 Congruences dans 17](#_Toc428346782)

[5.1 Définition 17](#_Toc428346783)

[5.2 Propriétés des congruences 18](#_Toc428346784)

[5.2.1 Transitivité de la congruence 18](#_Toc428346785)

[5.2.2 Compatibilité de la congruence avec l’addition membre à membre 19](#_Toc428346786)

[5.2.3 Compatibilité de la congruence avec la soustraction membre à membre 19](#_Toc428346787)

[5.2.4 Compatibilité de la congruence avec la multiplication membre à membre 20](#_Toc428346788)

[5.2.5 Compatibilité de la congruence avec les puissances 21](#_Toc428346789)

[5.3 Applications des congruences 22](#_Toc428346790)

CHAPITRE 1 : Divisibilité - Nombres premiers - Congruences

# Divisibilité dans

## Deux sortes de divisions

On distingue couramment deux types de divisions :

* La division « exacte »

Dividende

Quotient

Diviseur

* La **division euclidienne**[[1]](#footnote-1) appelée aussi **division entière** qui est une division « avec reste »

Dans l’antiquité, Euclide explique dans son ouvrage « Les éléments » comment diviser un dividende en faisant des soustractions successives.

***Exemple :***

*Comment partager équitablement 500 € entre* ***70 personnes****?*

* On prend 70 € que l’on répartit en donnant 1 € à chaque personne. Il reste 430 €
* On continue en prenant encore 70 € que l’on distribue aux 70 personnes. Celles-ci possèdent 2 € et il en reste 360…
* À la dernière étape, chaque personne possède 7 € et il en reste 10 que l’on ne peut plus partager si on respecte la règle qui veut qu’on ne calcule qu’avec des nombres entiers.

A chaque étape on peut écrire

qui sont des égalités correctes mais ne correspondent pas à une division euclidienne car la distribution n'est pas complète. Celle-ci est complète lorsque le **reste est strictement inférieur à 70**.

en vérifiant que

Dividende

Diviseur

Quotient

En [arithmétique](http://fr.wikipedia.org/wiki/Arithm%C3%A9tique), la **division euclidienne ou division entière** est une opération qui, à deux entiers appelés **dividende**  et **diviseur** , associe deux entiers appelés **quotient**  et **reste** . Initialement définie pour deux [entiers naturels](http://fr.wikipedia.org/wiki/Entier_naturel) non nuls, elle se généralise aux [entiers relatifs](http://fr.wikipedia.org/wiki/Entier_relatif).

Cette division est à la base des théorèmes de l'[arithmétique élémentaire](http://fr.wikipedia.org/wiki/Arithm%C3%A9tique_%C3%A9l%C3%A9mentaire). On peut aussi définir une division euclidienne sur d'autres ensembles comme l'ensemble des [polynômes](http://fr.wikipedia.org/wiki/Polyn%C3%B4me).

## Diviseurs

***Définition :***

On rappelle que l’ensemble des entiers relatifs

Soit un entier relatif et un entier relatif *non nul*.

**S’il existe un entier relatif**  tel que , alors  **divise**

On dit aussi : est divisible par ;  **est un diviseur de**  ; On note : et on lit ***b* divise *a.[[2]](#footnote-2)***

***Exemples :***

* Les diviseurs de sont :
* Les diviseurs de sont :
* Les **diviseurs communs** de et sont :
* Ainsi on a  ; ;;… ; ; ; ; ; etc.

***Propriétés :***

Soit et . Les propositions suivantes sont équivalentes :

***Démonstration  de l’équivalence :***

Les propositions suivantes sont équivalentes :

* Il existe tel que
* Il existe tel que

Les autres propositions équivalentes s’obtiennent avec la même méthode.

***Conséquence :***

* et ont les mêmes diviseurs dans
* Les diviseurs négatifs de sont les opposés des diviseurs positifs de .
* On étudie souvent seulement les diviseurs qui sont dans . On obtient facilement tous les diviseurs en prenant aussi leurs opposés.

***Propriété :***

Soit

Tout diviseur positif de est tel que

***Démonstration :***

Soit un entier et soit un diviseur de .

Donc, il existe tel que

Comme , on a

D’où . Tout diviseur strictement positif est inférieur ou égal à .

Ainsi, a au plus diviseurs dans .

Et donc, a au plus diviseurs dans .

***Conséquence :***

Tout a un nombre fini de diviseurs, tous compris entre et

***Remarques :***

* est vrai pour tout donc  **a comme diviseurs tous les entiers non nuls.**  
  Par exemple est un diviseur de car il existe un entier relatif tel que **()**
* Tout s’écrit . Donc tout entier relatif sauf 1, a au moins deux diviseurs dans :
* **a exactement un diviseur**

## Nombres premiers entre eux

***Définition :*** Deux entiers relatifs et **sont premiers entre eux[[3]](#footnote-3)** équivaut à :

et n’ont que **deux diviseurs communs** : et ou

***Exemple***  (qui a pour diviseurs ) et sont **premiers entre eux.**

***Remarques :***  **et** sont premiers avec tout entier. n’est premier avec aucun (sauf 1 et )

Pour tout et tout **, est irréductible** équivaut **à et sont premiers entre eux**.

## Transitivité de la division

Pour tous entiers , ,  : **Si divise et divise alors divise**

***Démonstration :***

D’après la définition de diviseur : Si  **est un diviseur** de alors il existe tel que

Si  **est un diviseur de**  alors il existe tel que

D’où :

est un entier relatif. Donc divise .

***Exemples :***

* divise 4 et divise donc divise
* Si divise , et puisque divise , alors divise .

## Divisibilité de toute combinaison linéaire par tout diviseur commun

On appelle *combinaison linéaire entière* des entiers et l’entier où et sont des entiers relatifs.

***Exemple :*** est une combinaison linéaire entière de et .

Pour tout , pour tout , pour tout  :

**Si** *c* est un diviseur communà et  **alors** *c* divise toute combinaison linéaire entière de la forme où et sont des entiers relatifs.

***Cas particuliers***

* *Cas :*  et Si divise et alors divise la somme

Par exemple, est un diviseur commun à et donc divise

* *Cas :*  et Si divise et alors divise la différence

Par exemple, est un diviseur commun à et donc divise

***Démonstration :***

Si est un diviseur commun à et alors d’après la définition de diviseur :

Il existe deux entiers relatifs et tels que et

Donc la combinaison linéaire s’écrit

est un entier relatif. Puisque alors **c divise**

***Exemple :***

* Soit un diviseur commun de et Proposer un ensemble dans lequel on est certain de trouver .

*Réponse :* **Si** **alors** divise également

Comme n’a que quatre diviseurs : 19 et , on en déduit que

# La division euclidienne de *a* par *b*

## Théorème sur l’existence et l’unicité d’un couple d’entiers naturels (*q* ; *r*)

Pour tout couple il ***existe*** un couple ***unique*** d’entiers naturels tels que

avec

* est le dividende (valeur à partager)
* est le diviseur (nombre de parts)
* est le quotient (valeur d’une part)
* est le reste (qui ne peut plus être divisé, toujours strictement inférieur au diviseur ).

***Exemple :***

Si et

Alors avec

Donc la division euclidienne associe au couple le couple

***Illustration graphique :***

Sur l’axe des multiples positifs de  :

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  |

On peut placer entre et

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  | |  |  | |  |  | |  | | | |  | |  |  |

***Remarque 1 :***

Parmi les multiples écritures , seule celle où est la relation de la division euclidienne de par

Seule, est *la relation de* *division euclidienne* de par car

***Remarque 2 :***

Pour trouver , on peut faire la division exacte de par . est la partie entière[[4]](#footnote-4) de

*Exemple :*

Si et alors la division euclidienne du dividende par donne le quotient .

***Remarque 3 :***

Comme la division euclidienne doit respecter la condition alors le reste ne peut prendre que valeurs possibles : tous les entiers de à

*Exemple :* dans la division par le reste peut prendre l’une des valeurs entières de à .

***Remarque 4 :***

La division de par a pour reste équivaut à divise (noté )

Par exemple, sietalorset divise (noté )

***Remarque 5 :***

Dans notre système de numération décimale, le chiffre des unités est le reste de la division euclidienne du nombre par 10.

*Exemple :* sietalorset(avec )

***Démonstration du théorème de la division euclidienne dans pour tout couple***

* Démontrons l’existence d’au moins un couple d’entiers naturels tels que .

La suite des multiples positifs de est : avec .

Si est divisible par , alors est un des termes de la suite ci-dessus. Donc dans ce cas on a avec . Donc et existent ( et ).

Si n’est pas divisible par alors il existe des multiples de inférieurs à et d’autres supérieurs à . Ainsi il existe un entier relatif tel que .

* Démontrons l’unicité du couple

On a vu qu’il existe au moins un couple d’entiers naturels vérifiant les deux conditions :

**et**

Alors en ajoutant aux trois membres de l’inégalité on a :

Soit . En divisant par on a

D’où, comme et sont deux entiers consécutifs, . Donc est unique et donc aussi.

## Division euclidienne dans

On a démontré que, dans tous les cas, étant donnés  *et* , il existe un couple d’entiers unique tels que .

On peut démontrer aussi que :

Etant donné  *et* , il existe un couple d’entiers unique tels que .

***Illustration graphique :***

Sur l’axe des réels gradué tous les avec (multiples de )

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  |

On place entre les multiples de consécutifs et

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  | |  |  | |  |  | |  | | | |  | | |  |

***Exemple  :***

Graduations : multiples de

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | |  | | | |  | |

Si et

Alors avec

Donc

## Propriétés de la relation de division euclidienne de *a* par *b*

Soit un couple divise si, et seulement, dans la division euclidienne de par , le reste .

On donne un entier naturel supérieur ou égal à .  
Tout entier relatif s’écrit sous l’une, et une seule, des formes suivantes :

***Exemple avec :***

Tout entier relatif s’écrit sous l’une, et une seule, des formes suivantes :

Par exemple, si on choisit , s’écrit

On donne un entier naturel supérieur ou égal à .  
Parmi entiers consécutifs, un et un seul est multiple de .

***Exemple avec  :***

Dans la suite des 70 entiers consécutifs , un et un seul est multiple de **70**.

***Autre exemple :***

Soit . Dans la suite , il y a un et un seul multiple de **5**.

# Les nombres premiers

## Définition d’un nombre premier

Un nombre premier est un naturel qui possède *exactement deux* diviseurs positifs : 1 et lui-même.

***Exemples :***

|  |  |  |  |
| --- | --- | --- | --- |
|  | Diviseurs positifs de | Nombre de diviseurs positifs | est-il premier ? |
|  |  | Une infinité | non |
|  |  |  | non |
|  |  |  | **oui** |
|  |  |  | **oui** |
|  |  |  | non |
|  |  |  | **oui** |
|  |  |  | non |

***Vocabulaire :***

Un nombre entier naturel supérieur ou égal à 2 non premier est dit *nombre composé*.

Par exemple, et sont composés.

***Remarques :***

1. Le plus petit nombre premier est . C’est le seul qui soit pair.
2. Les nombres premiers inférieurs ou égaux à sont  
    . il y en a . On note
3. Les nombres premiers ont une définition simple, mais peuvent conduire à des problèmes difficiles. Par exemple, la conjecture[[5]](#footnote-5) « Tout nombre **pair** différent de deux peut être décomposé en somme de deux nombres premiers » semble vraie, mais elle n’a pas encore été démontrée.
4. Ne pas confondre «  et sont des nombres premiers » et «  et sont des nombres premiers entre eux »

***Exemples*** :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | Diviseurs positifs de | Diviseurs positifs de | et sont premiers | Diviseurs positifs communs | et sont premiers entre eux |
|  |  |  |  | oui |  | non |
|  |  |  |  | oui |  | oui |
|  |  |  |  | non |  | non |
|  |  |  |  | non |  | oui |

1. Pour **tout nombre premier**  et pour tout , on est *dans l’une ou bien dans l’autre* des situations :

* divise
* est premier avec

***Exemples :***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | Diviseurs positifs de | Diviseurs positifs de | divise | et sont premiers entre eux |
|  |  |  |  | oui |  |
|  |  |  |  |  | oui |
|  |  |  |  | oui |  |
|  |  |  |  |  | oui |
|  |  |  |  |  | oui |
|  |  |  |  | oui |  |
|  |  |  |  |  | oui |
|  |  |  |  |  | oui |
|  |  |  |  |  | oui |
|  |  |  |  |  | oui |
|  |  |  |  |  | oui |
|  |  |  |  | oui |  |

## Théorème des diviseurs premiers

Pour tout , tel que on est *dans l’une ou bien dans l’autre* des situations :

* Si est premier alors admet **un seul diviseur premier : lui-même**
* Si est composé alors admet **au moins un diviseur premier**  qui vérifie la relation

Par exemple :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | Diviseurs positifs de | Diviseurs premiers de | admet un seul diviseur premier : lui-même | admet au moins un diviseur premier  tel que |
|  |  |  |  | oui |  |
|  |  |  |  | oui |  |
|  |  |  |  |  | oui |
|  |  |  |  | oui |  |
|  |  |  |  |  | oui |
|  |  |  |  | oui |  |
|  |  |  |  |  | oui |
|  |  |  |  |  | oui |
|  |  |  |  |  | oui |
|  |  |  |  | oui |  |
|  |  |  |  |  | oui |

***Remarque :*** Un entier peut avoir un diviseur premier supérieur à . Exemple :

***Démonstration du théorème des diviseurs premiers :***

Pour tout , tel que  :

* Si est premier alors admet exactement deux diviseurs : et lui-même. Mais comme n’est pas premier, alors admet bien un seul diviseur premier : lui-même.
* Si n’est pas premier alors admet d’autres diviseurs différents de et de lui-même avec

**1. Montrons que parmi ces diviseurs, le plus petit est premier :**

*Supposons* que soit composé, c'est-à-dire que a des diviseurs autres que est lui-même.

Si n’est pas premier alors admet d’autres diviseurs différents de et de lui-même avec

étant des diviseurs de qui est un des diviseurs de seraient aussi des diviseurs de

On aurait donc

et donc ne serait pas le plus petit des diviseurs de .

On voit que la *supposition* conduit à une contradiction. Donc elle est fausse.

Conclusion : , le plus petit des diviseurs de , est premier

Notons le plus petit diviseur premier de

**2. Montrons que, le plus petit diviseur est tel que :**

Cela équivaut à montrer que

On a où est un diviseur de

donc il existe aussi un diviseur de noté tel que où (puisque est le plus petit des diviseurs autres que )

On a donc

Conclusion :

* Dans le cas où n’est pas premier, il a au moins un diviseur premier tel que
* Dans le cas où n’est pas premier, le plus petit de ses diviseurs (différent de ) est premier.

## Tester la primalité

Soit un nombre supérieur ou égal à .

D’après le théorème des diviseurs premiers, si n’a aucun diviseur premier inférieur ou égal à alors est premier.

***Exemple :***

Tester la primalité de

Le test consiste à essayer de diviser par les premiers nombres premiers dans l’ordre croissant :

On sait que . Donc on ne cherchera pas si est divisible par un nombre premier strictement supérieur à

|  |  |  |
| --- | --- | --- |
|  |  | est divisible par |
|  | n’est pas pair | non |
|  | n’est pas un multiple de | non |
|  | ne se termine pas par ou | non |
|  | non divisible par | non |
|  | non divisible par | non |
|  |  | non |
|  |  | non |
|  |  | non |
|  |  | non |
|  |  | non |
|  |  | non |
|  |  | non |
|  |  | non |
|  |  | non |

Conclusion : est premier.

***Remarques :***

* Tester la primalité d’un nombre peut demander beaucoup de calculs.
* Pour obtenir un tableau de nombres premiers, plutôt que d’effectuer le test de primalité pour chaque nombre, on peut utiliser **un crible**, c'est-à-dire une méthode d’élimination en raisonnant par exemple avec les multiples.

Ainsi, le crible d’Eratosthène[[6]](#footnote-6) consiste à dresser un tableau des entiers naturels de à et à barrer puis les entiers multiples de sauf , puis les multiples de sauf , puis les multiples de sauf . Ainsi de suite. On barre les multiples des premiers nombres premiers en commençant par barrer . On s’arrête si est strictement supérieur à . Donc pour connaitre la primalité des entiers jusqu’à par exemple, il suffira de tester la primalité des entiers compris entre et car . On trouve nombres premiers inférieurs ou égaux à .

## Théorème sur l’infinité des nombres premiers

***Théorème :***

Il existe une infinité de nombres premiers.

***Démonstration :***

On considère les premiers nombres premiers

Soit l’entier

***Exemples :***

|  |  |  |
| --- | --- | --- |
|  |  | premier ? |
|  |  | oui |
|  |  | oui |
|  |  | oui |
|  |  | oui |
|  |  | oui |
|  |  | non[[7]](#footnote-7) |
|  |  | non[[8]](#footnote-8) |

**1. Cas où est premier**

Dans ce cas, comme est strictement supérieur au produit des premiers nombres premiers, nous obtenons un autre nombre premier que l’un des premiers nombres premiers considérés au départ. Donc on peut obtenir autant de nombres premiers que l’on veut. Autrement dit, il y a une infinité de nombres premiers.

**2. Cas où est composé. Montrons que l’un des facteurs de est un nombre premier différent des premiers nombres premiers**

D’après le théorème des diviseurs premiers, si est composé alors admet au moins un **diviseur premier**  (qui vérifie la relation ).

*Supposons* que soit l’un des premiers nombres premiers . Donc on peut écrire :

Comme n’est pas un entier alors la somme n’est pas un entier

ce qui est contradictoire avec le fait que est un entier.

On voit que la *supposition* conduit à une contradiction. Donc elle est fausse.

Conclusion : L’entier permet d’obtenir un nombre premier différent des premiers nombres premiers considérés au départ. Donc on peut obtenir autant de nombres premiers que l’on veut. Autrement dit, il y a une infinité de nombres premiers.

***Exemple :*** On peut trouver de très grands nombres premiers comme

***Remarque :*** Un nombre est un nombre de **Mersenne**. Les 4 premiers nombres de Mersenne sont premiers, mais la plupart comme ne le sont pas.

# Existence et unicité de la décomposition en facteurs premiers

## Théorème fondamental de l’arithmétique

* Pour tout entier naturel supérieur ou égal à **il existe** **une décomposition** en produit de facteurs premiers.
* Pour un entier donné, cette décomposition est **unique**, à l’ordre des facteurs près.

***Exemples :***

est premier. La décomposition est

n’est pas premier. On commence par déterminer le plus petit diviseur premier.

Ici, c’est

est aussi divisible par

etc.

On présente plus rapidement les calculs dans un tableau où apparaissent les diviseurs premiers dans l’ordre croissant :

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

La décomposition de est donc

La forme générale de la décomposition de est

où sont des nombres premiers distincts et où sont des entiers naturels non nuls

***Remarque :***

Tout entier supérieur ou égal à s’écrivant est divisible par et aussi par tout produit partiel de ses facteurs premiers. Par exemple est divisible par

De façon générale, est divisible par où sont des entiers naturels inférieurs ou égaux à

***Exemple :***

est divisible par

***Démonstration du théorème fondamental  de l’arithmétique :***

**1. Existence d’une décomposition de en produit de facteurs premiers**

D’après le théorème des diviseurs premiers :

Pour tout , tel que admet **au moins un diviseur premier**

* Lorsque est premier on a

D’où avec qui est premier. *Le théorème est démontré dans ce cas.*

* Lorsque est composé on a avec et

Comme est un entier strictement supérieur à , d’après le théorème des diviseurs premiers, admet **au moins un diviseur premier**

* + Lorsque est premier on a

D’où avec et qui sont premiers. *Le théorème est démontré dans ce cas*.

* + Lorsque est composé on a avec et

Comme est un entier strictement supérieur à , d’après le théorème des diviseurs premiers, admet **au moins un diviseur premier**

* + - Lorsque est premier on a

D’où avec et qui sont premiers. *Le théorème est démontré dans ce cas*

* + - Lorsque est composé on a avec et

Comme est un entier strictement supérieur à , d’après le théorème des diviseurs premiers, admet **au moins un diviseur premier**

On poursuit le même raisonnement tant que l’entier est composé. On obtient une suite d’entiers tels que .

La liste des entiers positifs est strictement décroissante et est minorée par Donc cette liste est finie la plus petite valeur éventuellement prise par étant qui est un nombre premier).

Donc au bout d’un nombre fini d’étapes, on aboutit à est premier et on a .

Donc dans tous les cas, on finit par obtenir la décomposition de en un produit fini de facteurs premiers :

**2. Unicité de la décomposition de en produit de facteurs premiers**

Soit un entier naturel

Supposons que ait deux décompositions en facteurs premiers :

et .

Alors l’un des **facteurs** , par exemple , **divise**  autrement dit, divise

Or est premier donc n’est pas composé. Donc n’est pas égal à un produit de facteurs premiers Mais est *égal à* l’un des facteurs premiers

En reprenant le raisonnement pour les autres facteurs premiers … on aboutit à la même conclusion. Ainsi la décomposition primaire d’un nombre entier naturel est unique.

## Théorème sur la forme des diviseurs

Pour tout entier naturel supérieur ou égal à il existe une décomposition unique en produit de facteurs premiers où sont des entiers naturels non nuls.

Tout diviseur positif de s’écrit sous la forme où sont des entiers naturels tels que

***Exemple :***

Soit . On décompose en facteurs premiers :

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Un diviseur de est par exemple

***Démonstration :***

**1. Montrons que si où sont des entiers tels que alors divise**

Comme les entiers sont tels que , alors il existe des entiers tels que ; ; … ;

et donc :

Conclusion : divise

**2. Réciproque : montrons que si divise alors où sont des entiers tels que**

divise alors où et sont des entiers tels que et .

Les entiers et se décomposent chacun en produit de facteurs premiers.

Le produit de ces produits est donc un produit de facteurs premiers égale à

D’après le théorème fondamental de l’arithmétique, la décomposition en facteurs premiers de est *unique*. Donc

Donc les facteurs premiers intervenant dans la décomposition du diviseur sont les nombres premiers avec une puissance inférieure ou égale à . Ce qui s’écrit :

avec tels que

Conclusion : Tout diviseur positif de s’écrit sous la forme où sont des entiers naturels tels que

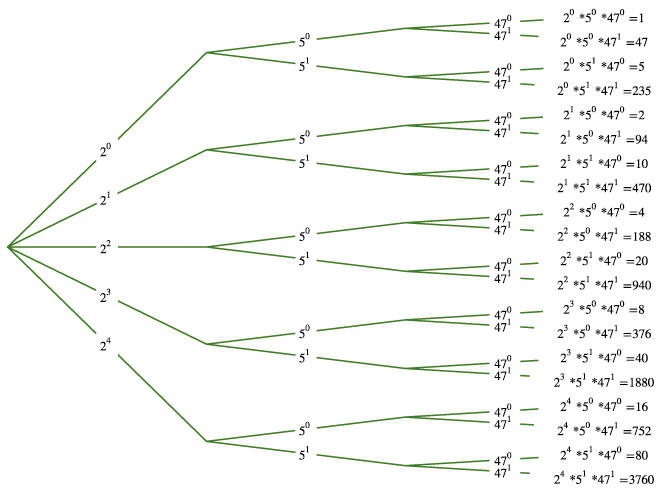
***Remarque :***

lorsque le nombre premier n’intervient pas dans la décomposition du diviseur

Par exemple pour , un des diviseurs est dans la décomposition duquel n’intervient pas.

## Nombre de diviseurs d’un entier naturel supérieur ou égal à 2

***Exemple :*** Reprenons **.** Les diviseurs de sont :

Pour obtenir tous les diviseurs de , on doit essayer toutes les listes de puissances avec .

On peut faire l’arbre des diviseurs :

Le nombre de diviseurs positifs de est :

De façon générale, **le nombre de diviseurs positifs** de est :

où sont des naturels non nuls.

***Remarque :*** a *diviseurs propres*[[9]](#footnote-9). La somme des diviseurs propres de est . Donc n’est pas un *nombre parfait*[[10]](#footnote-10).

# Congruences dans

## Définition

Soit . Pour tous couples d’entiers relatifs, il est équivalent de dire :

* et ont le même reste dans la division par
* est un multiple de (c'est-à-dire divise )
* et sont ***congrus*** ***modulo***

***Exemple :*** et 28 sont « congrus modulo  » car . On écrit

12 est le ***diviseur*** également appelé ***module***

Symbole introduit en 1801 par C. F. Gauss

avec

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |
|  |  | |  | |  | |  | |  | |  | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  |

***Illustration sur un cercle :***  Tous les entiers situés sur un même rayon sont congrus modulo 12.

***Exemples :***  donc

donc

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  | et | |
|  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  | pendule.bmp |  |  |  |  |  |  |  |  |  |  |  | | En multipliant **membre à membre** ou en additionnant membre à membre les entiers de 2 congruences modulo on obtient une congruence modulo |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | | et | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | **et** | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

et ne sont pas congrus modulo 12

et ne sont pas congrus modulo 12



## Propriétés des congruences

### Transitivité de la congruence

Soit . Pour tous entiers relatifs

Si et si alors

***Exemple :*** car

car

Donc, par transitivité,

avec

avec

avec

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |
|  |  | |  | |  | |  | |  | |  | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  |

***Remarques :***

* Soit . Tout entier relatif est congru à lui-même modulo   
  car
* car le reste dans la division par de ces deux entiers naturels est
* Soit . L’entier relatif est un multiple de équivaut à
* Soit et .   
  Si est le reste de la division euclidienne de par alors  Si  alors est le reste de la division euclidienne de par "  **est fausse** (cette proposition réciproque est vraie seulement si ).
* Les entiers relatifs congrus à modulo s’écrivent

***Exemple :*** les entiers relatifs congrus à modulo s’écrivent

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |
|  |  | |  | |  | |  | |  | |  | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  |

* Les entiers relatifs qui s’écrivent sont les entiers congrus à modulo , c'est-à-dire les entiers impairs.
* Soit . Pour tous couples d’entiers relatifs, il est équivalent de dire :
* divise
* Il existe un entier relatif tel que
* Il existe un entier relatif tel que

***Exemple :*** les entiers relatifs et sont congrus modulo 12 il existe tel que

### Compatibilité de la congruence avec l’addition membre à membre

Soit . Pour tous couples et d’entiers relatifs,

Si et si alors

***Démonstration :***

Si et si alors il existe deux entiers relatifs et tels que et

Donc en additionnant les deux égalités membre à membre :

est un entier relatif, donc

***Exemple :***

et donc

***Cas particulier :***

Soit . Pour tous entiers relatifs , si alors

***Exemple :***

donc

***Ainsi, on peut additionner aux deux membres le même entier dans les congruences.***

### Compatibilité de la congruence avec la soustraction membre à membre

Soit . Pour tous couples et d’entiers relatifs,

Si et si alors

***Démonstration :***

Si et si alors il existe deux entiers relatifs et tels que et

Donc en soustrayant les deux égalités membre à membre :

est un entier relatif, donc

***Exemple :***

et donc

***Cas particulier :***

Soit . Pour tous entiers relatifs et équivaut à

***Démonstration :***

Si et comme alors c'est-à-dire

Réciproquement, si et comme alors soit

***Exemple :***

équivaut à

***Ainsi, on peut « transposer » dans les congruences.***

### Compatibilité de la congruence avec la multiplication membre à membre

Soit . Pour tous couples et d’entiers relatifs,

Si et si alors

***Démonstration :***

Si et si alors il existe deux entiers relatifs et tels que et

Donc en multipliant les deux égalités membre à membre :

est un entier relatif, donc

***Exemple :***

et donc

***Cas particulier :***

Soit . Pour tous entiers relatifs , si alors

***Démonstration :***

On a vu que si et si alors

Or pour tout entier relatif , on sait que

Donc :

***Exemples :***

donc

donc pour tout

***Ainsi, on peut multiplier les deux membres par un même entier dans les congruences.***

***Conséquence pour les combinaisons linéaires d’entiers congrus modulo  :***

Soit . Pour tous couples et d’entiers relatifs, pour tous entiers relatifs et

Si et si alors

***Exemples :***

et donc   
d’où

et donc pour tous entiers et

 La congruence ***n’est pas compatible avec la division membre à membre***   
La proposition Si et si alors **est fausse**.

***Ainsi, on ne peut pas diviser les deux membres par un même entier k dans les congruences (sauf si on divise aussi le module c par k). Par exemple :***

***Contre exemples :***

La proposition donc est fausse.

La proposition donc est fausse.

La proposition donc est fausse.

### Compatibilité de la congruence avec les puissances

Soit . Pour tout couple d’entiers relatifs, et pour tout

Si alors

***Démonstration par récurrence :***

Dans toute cette démonstration, on suppose que l’hypothèse est vraie.

* Initialisation :

Pour

et

Si alors

D’où la proposition est vraie pour

* Hérédité :

On suppose que pour un certain entier naturel non nul on ait :

Montrons *qu’alors*

On a : (hypothèse de récurrence) et (hypothèse de départ)

D’après la compatibilité de la congruence avec la multiplication, on a :

D’où la proposition est héréditaire

* Conclusion :

Pour tous entiers relatifs et et pour tout entier naturel non nul , si alors

***Exemple :***

donc

***Conséquence pour les combinaisons linéaires de puissances d’entiers congrus modulo  :***

Soit . Pour tous couples et d’entiers relatifs, pour tous entiers naturels non nuls et

Si et si alors

***Exemples :***

et donc   
d’où

 La congruence ***n’est pas compatible avec les racines***   
La proposition Si alors **est fausse**.

***Contre exemple :***

La proposition " donc  " est fausse.

## Applications des congruences

***Exemple 1 :***

Montrer que pour tout l’entier est un multiple de

*Réponse :* On transforme la question de façon à utiliser les congruences :

est un multiple de équivaut à

On fait apparaitre une combinaison linéaire du type

Or, donc et donc

Donc pour tout , c'est-à-dire

et c'est-à-dire

Par compatibilité de la relation de congruence avec la multiplication :

et d’où et

Par compatibilité de la relation de congruence avec l’addition :

soit encore

***Exemple 2 :***

Montrer que pour tout l’entier est un multiple de

*Réponse :* On transforme la question de façon à utiliser la compatibilité de la congruence avec la multiplication. Le reste de la division de par 6 peut être 0, 1, 2, 3, 4, 5. Etudions les 6 cas :

* Premier cas : Le reste de la division de par est c'est-à-dire

Par compatibilité de la congruence avec l’addition, on a :

Par compatibilité de la congruence avec la multiplication, on a : donc :

Finalement : soit

On en déduit que dans le cas où est un multiple de

* On procède de même pour les autres cas, en simplifiant si possible.

Par exemple équivaut à car

* Les 6 cas sont résumés dans le tableau suivant :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Dans tous les cas, on obtient

Conclusion : pour tout , est un multiple de

On a étudié tous les cas possibles. C’est la méthode de ***disjonction des cas***. On dit aussi que c’est la méthode ***exhaustive***.

***Exemple 3 :***

Quel est le reste de la division de par ?

*Réponse :*

* On commence par transformer la question de façon à utiliser la congruence modulo 5 avec un nombre plus petit que  :

d’où

et donc,

* On cherche ensuite une puissance de qui soit congrue à **1** modulo 5

(cela permet d’utiliser la propriété

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Après quelques essais, on trouve

On fait apparaitre dans l’exposant on a

d’où

et donc,

Conclusion : le reste de la division de par est .

Une variante de cette méthode consiste à chercher une puissance qui soit congrue à -**1**

(On utilise la propriété

***Exemple 4 :***

Quel est le reste de la division par de ?

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Ou encore |  |  |

d’où

est impair donc

Donc on a avec d’où le reste de la division par de est **4**.

***Exemple 5 :***

Les propositions suivantes sont-elles vraies ?

1.

|  |
| --- |
| Soit . Pour tous entiers relatifs , , et pour tout entier relatif tel que , |

2.

|  |
| --- |
| Soit . Pour tous entiers relatifs , , et pour tout entier relatif tel que , |

*Réponse :*

Proposition 1 :

On a

Par compatibilité de la congruence avec la multiplication, on a

Et par transitivité de la congruence :

Si alors et Si alors

Conclusion : La proposition 1 est vraie

Proposition 2 :

On a

Par compatibilité de la congruence avec l’addition, on a

Et par transitivité de la congruence :

Si alors et Si alors

Conclusion : La proposition 2 est vraie

***Conséquence :***

***Dans une combinaison linéaire, on peut remplacer un ou plusieurs des termes ou facteurs par un autre qui lui soit congru. On obtient une relation de congruence équivalente.***

*Application numérique :*



équivaut successivement à :

* car et
* car

 Dire « pour tout ***équivaut à***   » **est faux**

car et ne sont pas congrus modulo pour tout

(Mais par compatibilité de la congruence avec les puissances « pour tout ***si*** ***alors***  » est vrai)

***Exemple 6 : Diverses manipulations sur les congruences***

|  |  |
| --- | --- |
| **Congru *à***  Soit et  se lit «  divise  »  et s’écrit avec les congruences :  ***Dans une congruence, est congru à modulo ,  si et seulement divise*** | *Exemple 1 :*  ( divise )  s’écrit avec les congruences :  *Exemple 2 :*  Pour tout  et pour tout on a  Ce qui s’écrit avec les congruences : |
| ***Utilisation de la* compatibilité *avec l’addition de***  Pour tout et pour tout on a  Donc  Equivaut successivement à  ***Dans une congruence, on peut ajouter à l’un des membres, un multiple du module*** | *Exemple :*  Pour tout  est un multiple de  Donc par exemple  Equivaut à |
| ***Utilisation de la* compatibilité *avec la multiplication par***  Pour tout et pour tout on a  Donc :  Equivaut successivement à  ***Dans une congruence, on peut multiplier l’un des membres, par un nombre congru à 1*** | *Exemple :*  Pour tout  Donc par exemple  Equivaut à |
| **Déduction d’une congruence modulo un diviseur du module**  Pour tous naturels non nuls et  et pour tous entiers relatifs et  :  ***Si alors***  C:\Documents and Settings\HP_Propriétaire\Local Settings\Temporary Internet Files\Content.IE5\MEK4C5F9\MC900411320[1].wmf La réciproque est *fausse*  *Exemples :*  Comme et a comme diviseurs Alors :   ; ;  ; | *Preuve :*  Equivaut à :  divise  Il existe tel que  *Donc*  Il existe tel que  divise |
| **Congruence modulo 2**   * équivaut successivement à * Il existe tel que * ***et ont la même parité*** | *Exemple :* Pour tous entiers *et :*    d’où  et ont la même parité |

1. **Euclide**, né vers -325, mort vers -265 à Alexandrie, est un mathématicien de la Grèce antique, auteur des *Éléments*, qui sont considérés comme l'un des textes fondateurs des mathématiques modernes. [↑](#footnote-ref-1)
2. Il est équivalent de dire que est un multiple de . [↑](#footnote-ref-2)
3. On dit aussi parfois «  et sont **étrangers** » [↑](#footnote-ref-3)
4. **Fonction partie entière** : Cette fonction notée associe à tout réel l’entier relatif immédiatement inférieur ou égal à . Par exemple,  ;  ; . Sur la calculatrice TI, pour avoir la partie entière de 500/70, aller dans **math**, menu NUM, 5 :partEnt(500/70) ou 5 :int(500/70) en anglais. [↑](#footnote-ref-4)
5. Cette conjecture fut émise par **Christian** **Goldbach**, mathématicien allemand, en 1742 [↑](#footnote-ref-5)
6. **Eratosthène**, 3ème siècle avant J-C. Mathématicien grec qui a vécu à Alexandrie. Il détermina que la Terre était ronde en calculant son diamètre à 12540 km (alors qu’en réalité il mesure 12760 km). [↑](#footnote-ref-6)
7. est divisible par [↑](#footnote-ref-7)
8. est divisible par [↑](#footnote-ref-8)
9. Les **diviseurs propres** (ou **diviseurs stricts**) d’un entier naturel sont tous ses diviseurs positifs y compris 1 sauf lui-même. [↑](#footnote-ref-9)
10. Un **nombre parfait** est un entier naturel égal à la somme de ses diviseurs propres. Par exemple, est parfait puisque est égal à la somme de ses diviseurs propres. Les nombres parfaits pairs sont liés aux nombres de Mersenne premiers. On connait 47 nombres parfaits (le plus petit est 6 et le plus grand connu est ). [↑](#footnote-ref-10)