Divisibilité et Congruences

1. Divisibilité dans 
   1. Quelques propriétés de 

*Théorème* : tout sous-ensemble non vide de  possède un plus petit élément.

*Démonstration* : c’est très dur ! On l’admet

*Corollaire*[[1]](#footnote-1) (principe de descente infinie) : il n’existe pas dans  de suite infinie strictement décroissante.

*Démonstration* à faire[[2]](#footnote-2) :

* 1. Notion de divisibilité

*Définition* : soient *a* et *b* deux entiers relatifs (c’est-à-dire dans ). S’il existe un entier relatif *k* tel que , on dit de manière équivalente que :

* *a* est un multiple de *b*;
* *b* est un diviseur de *a* ;
* *b* divise *a*.

On note .

*Remarques et propriétés immédiates :*

* 0 est un cas souvent problématique, ne pas oublier de le traiter, souvent à part.
* Pour tout entier relatif *a* de , les entiers  sont les multiples de *a*. L’ensemble de ces multiples est noté .

*Exemple* à compléter : 

* Tout entier relatif *a* admet des diviseurs, au moins  (si *a* ≠ 0 pour les deux derniers).
* Un entier naturel (de ) est un nombre premier si et seulement si il admet exactement deux diviseurs dans . Ceci exclut 0 et 1, qui ne sont pas premiers.
* Si *a* ≠ 0, tout diviseur *b* de *a* vérifie , car  avec .
* On en déduit immédiatement que tout entier non nul admet un nombre fini de diviseurs[[3]](#footnote-3).
  1. Propriétés

*Théorème* : soient *a,* *b* et *c* trois entiers relatifs.

* Si  alors  ;
* Si  alors  ;
* Si  et  alors :
  +  ;
  +  ;
  + et plus généralement *a* divise toute combinaison linéaire de *b* et *c* :

 , où *u* et *v* sont deux entiers relatifs quelconques.

* Si  et  alors .

*Démonstrations* : faire en exercice la preuve de la combinaison linéaire

*Théorème* : Si  et  alors *a* = *b*.

*Démonstration 1* :

Remarquons que *a* ≠ 0 (respectivement *b* ≠ 0), sinon  n’a pas de sens (respectivement). Puisque  et , il existe deux entiers relatifs *k* et  tels que  et .

Donc .

Comme *a* ≠ 0 et *b* ≠ 0, le produit *ab* est aussi différent de 0. On peut donc simplifier :



CQFD

*Démonstration 2* (plus élégante) :

Comme  et , alors d’après une des propriétés du § 1b/,  et .

Donc . ◼︎︎

* 1. Exemples et méthodes

*Récurrence* : Montrons que 

Initialisation : Pour *n* = 0,  et . La propriété est vraie au rang 0.

Hérédité : Supposons que pour un entier *n* fixé,  (hypothèse de récurrence)

Factorisons l’expression obtenue au rang *n* + 1, en faisant apparaître l’hypothèse de récurrence[[4]](#footnote-4) :

 (spoil 9 = 2 + 7)

D’après les propriétés du § 1c/, une combinaison linéaire de deux nombres divisibles par 7 est divisible par 7. Donc la propriété est vraie au rang *n* + 1.

Conclusion : la propriété étant initialisée et héréditaire, on a montré par récurrence que .

*Raisonnement par disjonction des cas*: montrons que 

* Soit *n* est pair, et alors il existe  tel que .

Donc  est divisible par 2

* Soit *n* est impair, et alors il existe  tel que .

Donc  est divisible par 2 ◼︎

*Utilisation de connaissances/astuces de calcul*: Montrons que .

Le cas *n* = 0 est trivial, supposons pour la suite *n* ≠ 0.



 d’après 

, qui est divisible par 4 par combinaison linéaire ◼︎

*Exercice* : reprendre les exemples 1 et 3 ci-dessus en échangeant les méthodes.

*Utilisation des propriétés du cours (divisibilité d’une combinaison linéaire ici, c’est très puissant)*

* Trouvons les entiers naturels *n* tels que *n* divise *n* + 8.

Comme  et  , alors . Donc , .

Le raisonnement précédent est une implication , il faut donc faire la réciproque.

Réciproquement, si , alors  est respectivement égal à 9, divisible par 1, puis 10, divisible par 2, puis 12 divisible par 8, et enfin 16, divisible par 8.

Donc 

* Trouvons les entiers naturels *n* tels que *n*– 4 divise 3*n* + 24. *A compléter !*

Même principe que le précédent, en un peu plus compliqué. Les détails sont laissés au lecteur.

 et  

Donc . Pourquoi a-t-on des nombres négatifs dans cet ensemble ? On en déduit ensuite les valeurs de *n* : 

Comme précédemment, on étudie la réciproque.

On peut le faire par combinaison linéaire également :

 et 

* Trouvons les entiers *a* tels que  et .

*A faire en s’inspirant des exemples précédents. Pour un des cas de la réciproque, il est plus simple de trouver un exemple où « ça marche ».*

* 1. La division euclidienne

*Théorème* : soient *a* et *b* deux entiers naturels non nuls[[5]](#footnote-5) (donc dans ).

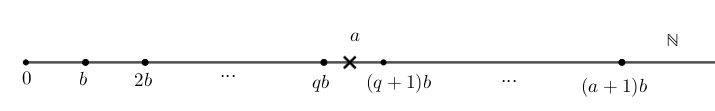
Alors il existe un unique couple  d’entiers naturels tels que .

*Vocabulaire*:

* Calculer *q* et *r* est effectuer la division euclidienne de *a* par *b*;
* *a* est le dividende ;
* *b* est le diviseur ;
* *q* est le quotient ;
* *r* est le reste.

*Démonstration* (essayez de la comprendre mais ne passez pas trop de temps dessus) :

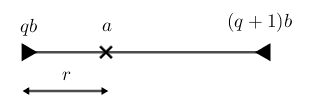
Existence : écrivons les multiples successifs de *b* sur un axe gradué :



On considère l’ensemble des multiples de *b* strictement supérieurs à *a*.

Comme , cet ensemble est non vide. D’après le théorème du § 1a, il admet un plus petit élément.

Supposons que cet élément soit .

Alors on a  (pourquoi n’a-t-on pas  ?)

Si  alors *r* = 0.

Sinon  . Posons dans ce cas .

D’une part, on a  car .

D’autre part  et  donne .

L’existence du couple  est prouvée.

Unicité : la preuve se fait par l’absurde, ce qui est souvent le cas pour l’unicité.

Supposons qu’il existe deux couples différents  et  tels que :

 et 

On obtient alors avec les encadrements sur les restes[[6]](#footnote-6) :  ;

Et avec en soustrayant les divisions euclidiennes  .

On en déduit que  est un multiple de b, qui est dans l’intervalle . le seul multiple de *b* dans cet intervalle est 0. Donc , que l’on notera *r* pour la suite.

On en déduit que  et  .

Donc . Comme *b* ≠ 0, on obtient en divisant par *b*: .

L’unicité est prouvée. ◼︎

*Théorème* : soient *a* un entier relatif, et *b* un entier naturel non nul.

Alors il existe un unique couple , avec *q* relatif et *r* naturel, tels que .

Le vocabulaire est le même que ci-dessus.

1. Les congruences

*Les congruences ne sont qu’une notation pratique pour la division euclidienne, et sa généralisation.*

* 1. Définition

*Définition* : soit *n* un entier naturel supérieur ou égal à 2, soient deux entiers relatifs *a* et *b*. 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 en général  , parfois ,  ou .

*Exemple* : l’heure de la sieste .

*Théorème* :

*Démonstration* : évidente, à faire quand même !

*Remarque* : on raisonne toujours avec des entiers lorsque l’on utilise des congruences.

* 1. Compatibilité avec les opérations

*Théorème* : soient *a,* *b*, *c* et *d* des entiers relatifs, *n* un entier naturel supérieur ou égal à 2, *p* un entier naturel quelconque.

Si  et  alors :

* 
* 
* 
* 

*Remarque* : et le quotient ?

*Démonstrations* :

* Pour  :

Comme  et , d’après le théorème du § 2a, il existe *k* et  tels que  et .

Donc . Toujours d’après le théorème du § 2a, ceci équivaut à .

* La preuve de  est quasi identique.
* Pour  , il faut adapter un peu… je vous laisse réfléchir ☺
* la preuve de  se fait par récurrence à partir du produit, faire au brouillon l’hérédité.

*Exemple* : il est 15 heures, quelle heure était-il il y a 173 heures ?

*Remarque et contre-exemples*: la propriété  n’est pas une équivalence.

*  mais 8 n’est pas congru à 10 (ni à -10 si on pense à  ) modulo 36.
*  mais 8 n’est pas congru à 11 (ni à -11 si on pense à  ) modulo 36
  1. Exemples et méthodes

*Bien sûr, la calculatrice est interdite…*

* Quel est le reste de  dans la division euclidienne par 7 ?

On remarque que  , le reste vaut 1.

* Quel est le reste de  dans la division euclidienne par 7 ?

On cherche une puissance de 23 congrue à 1 modulo 7.

On part de .

On en déduit que  puis .

On effectue la division euclidienne de l’exposant 41 par la puissance trouvée 3 : 

D’où  . Le reste est 4.

* Avec des entiers négatifs dans les congruences : montrer que  est divisible par 5. Généraliser.

On a :

* + 
  + 
  +  → on a remarqué que 
  + 

D’où 

* + Généralisation ?

1. Une application : critères de divisibilité

On note les entiers avec une barre par dessus pour faire apparaître leur décomposition dans le système décimal (base 10) :  .

Pour trouver un critère de divisibilité, on simplifie l’écriture d’un nombre grâce aux congruences modulo le diviseur.

*Exemples*:

* Critère de divisibilité par 9

Comme  , puis  par puissance, on en déduit que



Donc un entier est divisible par 9 si la somme de ses chiffres est divisible par 9

* Critères de divisibilité par 3 et par 5 : *à faire sur le modèle du critère de divisibilité par 9*
* Critère de divisibilité par 4

Comme  , puis  pour *n* ≥ 2 par produit, on en déduit que



Donc un entier est divisible par 4 si et seulement si le nombre composé de ses deux derniers chiffres est divisible par 4.

*raisonnement similaire pour la divisibilité par 8*.

* Critère de divisibilité par 11

Comme  et  , on en déduit que  et  d’où



Donc un entier est divisible par 11 si la somme alternée de ses chiffres est divisible par -11

* Critère de divisibilité par 7, par 13, … : ça se complique ! mais on peut toujours raisonner comme ci-dessus.

*Une autre méthode pour un critère pour la divisibilité par 7* : montrer que si un entier *n* de la forme  est divisible par 7, alors le nombre  est divisible par 7 (*indice* : se fait en une seule congruence par produit)

*Application*: pour 25718, itérer le processus jusqu’à obtenir un nombre simple.

Cours de Frédéric Mandon sous licence Creative Commons BY NC SA, <https://creativecommons.org/licenses/by-nc-sa/3.0/fr/>

1. Un corollaire est la conséquence « facile » d’un théorème principal. Un lemme est un petit théorème qui sert à démontrer un gros théorème. [↑](#footnote-ref-1)
2. Preuve qui tient en une ligne… [↑](#footnote-ref-2)
3. Constatez comme une propriété aussi évidente n’est pas si simple à démontrer. [↑](#footnote-ref-3)
4. L’idée est de forcer la factorisation sur un des deux termes du rang *n* + 1, et de voir ce qu’il reste ou ce qu’il faut enlever. Faites le calcul en factorisant par 9 et non par 2 : vous constaterez que la méthode fonctionne tout aussi bien. [↑](#footnote-ref-4)
5. La définition reste juste avec simplement *b* ≠ 0, mais n’a que peu d’intérêt dans ce cas. [↑](#footnote-ref-5)
6. Attention : on ne soustrait jamais deux encadrements. On passe à l’opposé sur le deuxième encadrement, et on ajoute les encadrements obtenus [↑](#footnote-ref-6)