DIVISIBILITÉ ET CONGRUENCES

I. Divisibilité dans

Définition : Soit *a* et *b* deux entiers relatifs.

*a* **divise** *b* s'il existe un entier relatif *k* tel que *b* = *ka.*

On dit également :

- *a* est un **diviseur** de *b,*

- *b* est **divisible** par *a,*

- *b* est un **multiple** de *a.*

Notation : divise se note : ∣

Exemples :

* 56 est un multiple de –8 car 56 = –7 x (–8)
* L'ensemble des multiples de 5 sont {… ; –15 ; –10 ; –5 ; 0 ; 5 ; 10 ; …}. On note cet ensemble .
* L’ensemble des diviseurs de 6 sont {–6 ; –3 ; –2 ; –1 ; 1 ; 2 ; 3 ; 6}
* 0 est divisible par tout entier relatif.

Propriété (transitivité) : Soit *a* et *b* deux entiers relatifs avec *b* non nul.

*b* divise *a* –*b* divise *a* *b* divise –*a* –*b* divise –*a*

Propriété (transitivité) : Soit *a*, *b* et *c* trois entiers relatifs.

Si *a* divise *b* et *b* divise *c* alors *a* divise *c*.

Démonstration :

Si *a* divise *b* et *b* divise *c* alors il existe deux entiers relatifs *k* et *k'* tels que *b* = *ka* et

*c* = *k'b.*

Donc *c* = *k’ka* et donc il existe un entier relatif *l* = *kk*' tel que *c* = *la.*

Donc *a* divise *c*.

Exemple :

* 3∣12 et 12∣36 donc 3∣36.
* On peut appliquer également la contraposée de la propriété de transitivité :

Comme 2 ne divise pas 1001, aucun nombre pair ne divise 1001.

En effet, si par exemple 10 divisait 1001 alors 2 diviserait 1001.

Méthode : Appliquer la définition de la divisibilité (démonstration par l’absurde)

 **Vidéo** [**https://youtu.be/z-CtTbP3RYA**](https://youtu.be/z-CtTbP3RYA)

Démontrer que pour tout entier relatif , le nombre n’est pas divisible par 3.

On va effectuer un raisonnement par l’absurde en supposant le contraire de ce qu’il faut démontrer.

Si notre démonstration aboutit à une « absurdité », une contradiction, cela prouvera que notre hypothèse de départ est fausse.

Supposons, *par l’absurde*, qu’il existe un entier relatif , tel que soit divisible par 3.

Il existe alors un entier relatif tel que

Soit : , soit encore : .

Ce qui signifie que 5 est divisible par 3. C’est « absurde », donc l’hypothèse de départ est fausse.

Le nombre n’est pas divisible par 3

Propriété (combinaisons linéaires) : Soit *a*, *b* et *c* trois entiers relatifs.

Si *c* divise *a* et *b* alors *c* divise *ma* + *nb* où *m* et *n* sont deux entiers relatifs.

Démonstration :

Si *c* divise *a* et *b* alors il existe deux entiers relatifs *k* et *k'* tels que *a* = *kc* et

*b* = *k'c.*

Donc *ma + nb* = *mkc + nk'c* et donc il existe un entier relatif *l* = *mk + nk*' tel que

*ma + nb* = *lc.*

Exemple :

Soit un entier relatif qui divise les entiers relatifs et .

Alors divise . Donc ou .

Méthode : Utiliser la propriété des combinaisons linéaires (démonstration avec réciproque)

 **Vidéo** [**https://youtu.be/JGJ0VJV2Zgo**](https://youtu.be/JGJ0VJV2Zgo)

Déterminer les entiers relatifs , tels que divise .

* On a :

**Si** et , **alors** d’après la propriété des combinaisons linéaires :

L’idée est de fabriquer une combinaison linéaire de et qui ne dépende plus de .

Soit :

Soit encore : .

Les diviseurs de 7 sont : –7 ; –1 ; 1 et 7.

Donc :

soit

soit

soit

soit

Les solutions possibles appartiennent à l’ensemble {–6 ; –3 ; –2 ; 1}.

Attention, il faut maintenant vérifier la réciproque. En effet, la propriété des combinaisons linéaires (si… alors…) donne une condition nécessaire pour avoir la divisibilité sur les combinaisons linéaires.

On a donc prouvé que, si divise , alors nécessairement appartient à l’ensemble {–6 ; –3 ; –2 ; 1}. La question est maintenant de savoir s’il suffit de prendre une valeur dans cet ensemble pour que divise .

Il faut donc prouver maintenant que si appartient à l’ensemble {–6 ; –3 ; –2 ; 1} alors divise

* Si  :

et . Or, , donc est bien solution.

Si  :

et . Or, , donc est bien solution.

Si  :

et . Or, , donc est bien solution.

Si  :

et . Or, , donc est bien solution.

* Les solutions sont –6, –3, –2 et 1.

II. Division euclidienne

Propriété : Soit *a* un entier naturel et *b* entier naturel non nul.

Il existe un unique couple d’entiers (*q* ; *r*) tel que *a* = *bq* + *r* avec .

Définitions :

- *q* est appelé le **quotient** de la division euclidienne de *a* par *b*,

- *r* est appelé le **reste**.

Exemple :

Dans la division euclidienne de 412 par 15, on a : 412 = 15 x 27 + 7

Démonstration :

**Existence :**

1er cas : : Le couple (*q* ; *r*) = (0 ; *a*) convient.

2e cas : : Soit *E* l'ensemble des multiples de *b* strictement supérieurs à *a*.

Alors *E* est non vide car l'entier appartient à *E*.

En effet donc .

*E* possède donc un plus petit élément c'est à dire un multiple de *b* strictement supérieur à *a* tel que le multiple précédent soit inférieur ou égal à *a*.

Il existe donc un entier *q* tel que .

Comme, on a : .

Et comme , on a : et donc .

*q* est donc un entier naturel.

On peut poser .

Or *a*, *b* et *q* sont des entiers, donc *r* est entier.

Comme , on a donc *r* est donc un entier naturel.

Et comme on en déduit que .

**Unicité :**

On suppose qu'il existe deux couples (*q* ; *r*) et (*q'* ; *r'*).

Donc .

Et donc : .

Comme est entier, est un multiple de *b*.

On sait que et donc et ,

donc .

Le seul multiple de *b* compris entre –*b* et *b* est 0, donc et donc *.*

D'où .

Propriété : On peut étendre la propriété précédente au cas où *a* est un entier relatif.

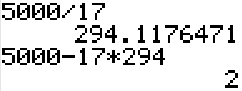
*- Admis -*

Méthode : Déterminer le quotient et le reste d'une division euclidienne (1)

 **Vidéo** [**https://youtu.be/bwS45UeOZrg**](https://youtu.be/bwS45UeOZrg)

Déterminer le quotient et le reste de la division de –5000 par 17.

A l'aide de la calculatrice, on obtient :



Ainsi : 5000 = 17 x 294 + 2

Donc : –5000 = 17 x (–294) – 2

Le reste est un entier positif inférieur à 17.

Donc : –5000 = 17 x (–294) – 17 – 2 + 17

Soit : –5000 = 17 x (–295) + 15

D'où, le quotient est –295 et le reste est 15.

Méthode : Déterminer le quotient et le reste d'une division euclidienne (2)

 **Vidéo** [**https://youtu.be/fv5uhr8JP3U**](https://youtu.be/fv5uhr8JP3U)

Déterminer le quotient et le reste de la division de par , avec entier naturel.

* Pour tout entier naturel , on a :

On décompose en .

On a choisi car est le plus grand facteur entier tel que . En effet, le produit du diviseur par le quotient ne doit pas dépasser le dividende, sinon le reste serait négatif !

La relation est la division euclidienne de par à condition que , soit : ou encore .

Ainsi, pour , dans la division euclidienne de par , le quotient est et le reste est .

* Reste donc à traiter les cas et

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | Quotient | Reste |
| 0 | 11 | 3 | 3 | 2 |
| 1 | 16 | 5 | 3 | 1 |
| 2 | 21 | 7 | 3 | 0 |

Propriété : Soit un entier naturel , tel que .

Alors, tout entier s’écrit sous l’une des formes suivantes :

ou ou … ou , avec entier relatif.

Exemples pour comprendre :

- En effectuant la division de par , on a : , avec .

Ainsi, peut s’écrire : ou ou ou ou .

- De même, peut s’écrire : ou .

On retrouve ici, la notion de parité d’un nombre : un nombre est soit pair, soit impair.

Méthode : Effectuer une démonstration par disjonction des cas

 **Vidéo** [**https://youtu.be/AEkdYp0Dqso**](https://youtu.be/AEkdYp0Dqso)

Démontrer que pour tout entier naturel , est divisible par 3.

Le raisonnement par disjonction de cas consiste à décomposer la proposition que l'on veut démontrer en différents cas qui seront vérifiés successivement.

On veut démontrer ici une divisibilité par 3, il peut donc être pertinent de décomposer l’entier sous une des trois formes suivantes :

ou ou , avec entier relatif.

On a donc 3 cas possibles :

* Si  :

donc est divisible par 3.

* Si  :

donc est divisible par 3.

* Si  :

donc est divisible par 3.

Ainsi, pour tout entier naturel , est divisible par 3.

III. Congruences dans

1) Définition

Exemple :

On considère la suite de nombres : 1, 6, 11, 16, 21, 26, 31, 36.

Si on prend deux quelconques de ces nombres, alors leur différence est divisible par 5.

Par exemple : 21 – 6 = 15 qui est divisible par 5.

On dit que 21 et 6 sont congrus modulo 5.

Définition : Soit *n* un entier naturel non nul.

Deux entiers *a* et *b* sont congrus modulo *n* lorsque *a* – *b* est divisible par *n*.

On note .

Propriété : Soit *n* un entier naturel non nul.

Deux entiers *a* et *b* sont congrus modulo *n*, si et seulement si, la division euclidienne de *a* par *n* a le même reste que la division euclidienne de *b* par *n*.

Démonstration :

- Si *r* = *r'* :

*a* – *b* = *nq* + *r* – *nq'* – *r'* = *n*(*q* – *q'*) donc *a* – *b* est divisible par *n* et donc .

- Si *a* et *b* sont congrus modulo *n* :

*a* – *b* = *nq* + *r* – *nq'* – *r'* = *n*(*q* – *q'*) + *r* – *r'*

Donc *r* – *r'* = *a* – *b* – *n*(*q* – *q'*)

Comme , *a* – *b* est divisible par *n* et donc *r* – *r'* est divisible par *n.*

Par ailleurs, et

Donc et

Et donc .

*r* – *r'* est un multiple de *n* compris entre –*n* et *n* donc , soit *.*

Exemple : On a vu que .

Les égalités euclidiennes 21 = 4 x 5 + 1 et 6 = 1 x 5 + 1 montrent que le reste de la division de 21 par 5 est égal au reste de la division de 6 par 5.

Méthode : Écrire avec des congruences

 **Vidéo** [**https://youtu.be/BTCsGN6xwXg**](https://youtu.be/BTCsGN6xwXg)

 **Vidéo** [**https://youtu.be/wdFNCnSfIgE**](https://youtu.be/wdFNCnSfIgE)

1) Compléter :

2) Démontrer que :

1) – Les solutions sont multiples, la plus simple consisterait à écrire  !

Ce n’est évidemment pas satisfaisant, on privilégiera la recherche d’un entier naturel tel que **avec** (en référence à la division euclidienne).

En effet, si est le reste de la division de 13 par 5, alors on a : .

signifie que , soit , .

On cherche donc un entier relatif , tel que .

En prenant , on a : .

Ainsi : .

– On cherche , tel que et .

signifie que , .

Avec , on trouve .

Ainsi : .

– On cherche , tel que et .

signifie que , .

Avec , on trouve .

Ainsi : .

2) signifie qu’il existe un entier relatif , tel que .

C’est vrai !

En effet, convient :

2) Propriétés sur les congruences

Propriétés : Soit *n* un entier naturel non nul.

a) pour tout entier relatif *a*.

b) Si et alors (Relation de transitivité)

Démonstration :

a) *a* – *a* = 0 est divisible par *n*.

b) et donc *n* divise *a* – *b* et *b* – *c* donc *n* divise *a* – *b* + *b* – *c* = *a* – *c*.

Propriété (Opérations) : Soit un entier naturel non nul.

Soit *a*, *b*, *a'* et *b'* des nombres relatifs tels que et **alors** on a :

-

-

-

- avec .

Démonstration de la dernière relation :

* Initialisation : La démonstration est triviale pour *p* = 0 ou *p* = 1
* Hérédité :

- Hypothèse de récurrence :

Supposons qu'il existe un entier *k* tel que la propriété soit vraie :

- Démontrons que : La propriété est vraie au rang : .

* Conclusion :

La propriété est vraie pour *p* = 0 et héréditaire à partir de ce rang. D'après le principe de récurrence, elle est vraie pour tout entier naturel *p*.

Exemples :

On a : et donc :

- et on a alors

- et on a alors

Attention la réciproque est fausse :

Si , on n’a pas nécessairement .

Méthode : Appliquer les propriétés sur les congruences

 **Vidéo** [**https://youtu.be/4RRjMC8\_Dio**](https://youtu.be/4RRjMC8_Dio)

Compléter le tableau :

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

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

3) Exemples d’application

Méthode : Résoudre une équation avec des congruences

 **Vidéo** [**https://youtu.be/Hb39SqG6nbg**](https://youtu.be/Hb39SqG6nbg)

 **Vidéo** [**https://youtu.be/aTn05hp\_b7I**](https://youtu.be/aTn05hp_b7I)

a) Déterminer les entiers *x* tels que

b) Déterminer les entiers *x* tels que

a)

Les entiers *x* solutions sont tous les entiers de la forme avec .

b) donc

Or *x* est nécessairement congru à l'un des entiers 0, 1, 2 ou 3 modulo 4.

Par disjonction des cas, on a :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *x* modulo 4 | 0 | 1 | 2 | 3 |
| 3*x* modulo 4 | 0 | 3 | 2 | 1 |

Donc On en déduit que .

Les entiers *x* solutions sont tous les entiers de la forme avec .

Méthode : Démontrer une divisibilité à l’aide des congruences

 **Vidéo** [**https://youtu.be/ZzlPFO59\_t0**](https://youtu.be/ZzlPFO59_t0)

Démontrer que pour tout entier naturel , est divisible par 3.

*On retrouve le même exercice (résolu ici à l’aide des congruences) que celui proposé dans le paragraphe II.*

On veut démontrer ici une divisibilité par 3, il peut donc être pertinent d’écrire à l’aide de modulo 3 :

ou ou

On a donc 3 cas possibles, on va effectuer la démonstration par disjonction des cas en présentant les calculs dans un tableau :

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

Ainsi, pour tout entier naturel , est divisible par 3.

Méthode : Déterminer le reste d'une division euclidienne à l'aide de congruences

 **Vidéo** [**https://youtu.be/uVS-oeibDJ4**](https://youtu.be/uVS-oeibDJ4)

a) Déterminer le reste de la division de 2456 par 5.

b) Déterminer le reste de la division de 2437 par 7.

a) Toute puissance de 1 est égale à 1. On cherche donc à faire apparaitre une puissance de 2 qui est égale à 1 modulo 5.

On choisit alors de décomposer 456 à l'aide du facteur 4 car .

On applique la formule de congruence des puissances :

Le reste est égal à 1.

b) On cherche donc une puissance de 2 qui est égale à 1 modulo 7.

On choisit alors de décomposer 437 à l'aide du facteur 3 car .

Le reste est égal à 4.

**Étude d’un problème de chiffrement : Appliquer un codage (Cryptographie) :**

 **Vidéo** [**https://youtu.be/GC7lFz4WGsc**](https://youtu.be/GC7lFz4WGsc)



Hors du cadre de la classe, aucune reproduction, même partielle, autres que celles prévues à l'article L 122-5 du code de la propriété intellectuelle, ne peut être faite de ce site sans l'autorisation expresse de l'auteur.

[*www.maths-et-tiques.fr/index.php/mentions-legales*](http://www.maths-et-tiques.fr/index.php/mentions-legales)