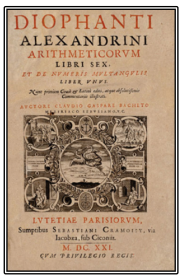
Divisibilité et congruence

Compétences attendues en fin de chapitre :

- Divisibilité dans $\mathbb{Z}$.
- Déterminer les diviseurs d'un entier. PGCD de deux entiers. Algorithme d'Euclide.
- Résoudre une congruence $ax \equiv b[n]$. Déterminer un inverse de a modulo n lorsque a et n sont premiers entre eux.

Le mathématicien du chapitre :



Diophante d'Alexandrie est un mathématicien de langue grec qui a vécu entre le III^{ème} et II^{ème} siècle avant JC. Il est parfois surnommé le père de l'Algèbre. Son ouvrage le plus important est Arithmétiques. Les applications importantes de son héritage sont nombreuses :la sécurité informatique, le chiffrement RSA ou encore les codes-barres. L'équation $ax + by = c$ permet notamment de déterminer la validité des codes-barres.

On rappelle que $\mathbb{N}$ est l'ensemble des entiers naturels, c'est-à-dire $\{0\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ \dots\}$
On rappelle que $\mathbb{Z}$ est l'ensemble des entiers relatifs, c'est-à-dire $\{\dots\ ;\ -2\ ;\ -1\ ;\ 0\ ;\ 1\ ;\ 2\ ;\ \dots\}$

1) Divisibilité dans $\mathbb{Z}$

Définition :

Soient a et b deux entiers relatifs avec b non nul. On dit que b divise a ou que ou que b est un diviseur de a s'il existe un entier relatif k tel que $a = bk$.
On dit aussi que a est un multiple de b.

Remarques :

- Attention, le diviseur n'est plus nécessairement plus petit que le nombre.
- 0 est un multiple de n'importe quel entier relatif. En effet, $0 = 0 \times k$
- 0 n'est un diviseur d'aucun nombre.

Exemples :

- 6 divise 42 car $42 = 6 \times 7$ comme au collège.
- -5 divise 35 car $35 = -5 \times (-7)$
- -28 divise -56 car $-56 = -28 \times 2$. Le diviseur est plus grand que le nombre.

Propriété :

Soient a et b deux entiers relatifs avec b non nul. On a alors :

- Si b divise a, alors les multiples de a sont des multiples de b.
- Si b divise a, alors les diviseurs de b sont des diviseurs de a.

Remarque :

- L'ensemble des multiples d'un entier relatif b dans $\mathbb{Z}$ est noté $b\mathbb{Z}$.
- L'ensemble des diviseurs d'un entier relatif b dans $\mathbb{Z}$ est noté $D(b)$

Ainsi, si b divise a, alors $a\mathbb{Z} \subset b\mathbb{Z}$ et $D(b) \subset D(a)$. C'est la raison pour laquelle la table de 6 est inclue dans la table de 3.

Exercice :

Montrer que $15p^2 - 35q$ est divisible par 5 quels que soient les entiers relatifs p et q.

Solution :

On factorise $15p^2 - 35q = 5(3p^2 - 7q)$ p et q étant des entiers relatifs, alors $3p^2 - 7q$ aussi
On a donc bien que $15p^2 - 35q$ est divisible par 5

Exercice :

Montrer que $3n + 5$ n'est jamais divisible par 3.

Solution :

On raisonne par l'absurde en supposant que $3n + 5$ est divisible par 3. Il existe donc $k \in \mathbb{Z}$ tel que $3n + 5 = 3k \Leftrightarrow 3(n - k) = -5$. Ceci est impossible car 5 n'est pas un multiple de 3.

Propriété :

Soient a et b deux entiers relatifs avec b non nul. On a alors :
b divise $a \Leftrightarrow -b$ divise $a \Leftrightarrow b$ divise $-a \Leftrightarrow -b$ divise $-a$

Conséquence :

a et $-a$ ont les mêmes diviseurs dans $\mathbb{Z}$

Propriété :

Tout entier relatif non nul a possède un nombre fini de diviseurs compris entre $-a$ et a

```
1   def diviseurs(n):
2     L=[]
3     for i in range(1,n+1):
4       if n%i==0:
5         L.append(i)
6     return L
```

```
> diviseurs(10)
[1, 2, 5, 10]
> diviseurs(28)
[1, 2, 4, 7, 14, 28]
> diviseurs(7)
[1, 7]
```

Exercice :

Déterminer l'ensemble des diviseurs de 28.

Solution :

On cherche dans l'ordre parmi tous les entiers inférieurs à 28. On obtient :
$D(28) = \{-28; -14; -7; -4; -2; -1; 1; 2; 4; 7; 14; 28\}$
On observe la symétrie de l'ensemble des diviseurs autour de 0.

Propriété :

Soient a, b et c des entiers relatifs avec a et b non nul.

- Si a divise b et b divise c, alors a divise c. La relation est transitive.
- Si a divise b et c, alors a divise toute combinaison linéaire de la forme $bu + cv$ où u et v sont deux entiers relatifs

Exemple :

Si a divise deux entiers consécutifs n et $n + 1$, alors a divise $(n + 1) - n = 1$
Donc a divise 1. Ainsi $a = 1$ou $a = -1$

2) *Division Euclidienne*

Théorème :

Soient a un entier relatif et b un entier naturel non nul.
Il existe un unique couple d'entiers relatifs $(q; r)$ tels que $a = bq + r$ avec $0 \leq r < b$.
q est le quotient et r le reste de la division euclidienne de a par b.

Remarques :

- Ce qui change avec le collège, c'est que a peut être négatif…
- Dans la division euclidienne par b, il y a b restes possibles qui sont $[|0; b - 1|]$.
- Il existe une infinité d'écriture $a = bq + r$ mais la contrainte du reste donne l'unicité de l'écriture.
- Si a est négatif, alors q l'est aussi.
- Si le reste est nul, on dit que b divise a.

Exemple :

- $115 = 7 \times 16 + 3$ est une division euclidienne.
- $115 = 7 \times 14 + 17$ n'est pas une division euclidienne.
- $-115 = 7 \times (-17) + 4$ est une division euclidienne.
- $217 = 7 \times 31 + 0$ est une division euclidienne

Exercice :

Soit n un entier naturel non nul. Déterminer suivant les valeurs de n le quotient et le reste de la division euclidienne de $7n + 5$ par $3n + 1$.

Solution :

On écrit naturellement l'égalité $a = bq + r$ soit $7n + 5 = (3n + 1) \times q + r$
On a intuitivement que $7n + 5 = (3n + 1) \times 2 + n + 3$ avec la contrainte du reste représentée par : $0 \leq n + 3 < 3n + 1 \Leftrightarrow n > 1$
Ainsi, si $n > 1$, le reste vaut $n + 3$.

Propriété :

Soit b un entier naturel supérieur ou égal à 2.
Tout entier relatif s'écrit sous l'une des formes suivantes :
$bq\ ; bq + 1\ ; bq + 2\ ; \ldots ; bq + (b - 1)$ où q est un entier relatif.

Démonstration :

Soit a un entier. En effectuant la division euclidienne de a par b non nul, il existe deux entiers$(q; r)$ tels que $a = bq + r$ avec $0 \leq r < b$. Par unicité du quotient et du reste, nous avons les possibilités $a = bq$ ou $a = bq + 1$ ou … $a = bq + (b - 1)$

Exercice :

Montrer que $(n^2 + 1)$ n'est jamais divisible par 3.

Solution :

On raisonne par disjonction de cas. Pour cela on utilise les écritures possibles de n dans la division euclidienne par 3. Soit $n = 3q$, soit $n = 3q + 1$, soit $n = 3q + 2$ avec $q \in \mathbb{Z}$.

- Si $n = 3q$, alors $n^2 + 1 = 9q^2 + 1$ et $n^2 + 1$ n'est pas divisible par 3.
- Si $n = 3q + 1$, alors $n^2 + 1 = 3(3q^2 + 2q) + 2$ et $n^2 + 1$n'est pas divisible par 3.
- Si $n = 3q + 2$, alors $n^2 + 1 = 3(3q^2 + 4q) + 5$ et $n^2 + 1$n'est pas divisible par 3.

Ainsi, $(n^2 + 1)$ n'est jamais divisible par 3

3) Congruence dans $\mathbb{Z}$

a) Définitions

Propriété :

Soient a et b deux entiers relatifs et n entier naturel non nul.
On dit que a est congru à b modulo n lorsque $a - b$ est un multiple de n.
On note :$a \equiv b[n]$ ou aussi $a \equiv b\ mod(n)$

Exemple :

$15 - 7 = 2 \times 4$ donc $15 \equiv 7[4]$ mais aussi $15 \equiv 7[2]$

Propriété :

Soient a et b deux entiers relatifs et n entier naturel non nul.
a est congru à b modulo n si et seulement si a et b ont le même reste dans la division euclidienne par n.

Exemple :

$11 = 4 \times 2 + 3$ donc $11 \equiv 3[4]$ mais puisque $7 = 4 \times 1 + 3$, $7 \equiv 3[4]$.
Et donc $11 \equiv 7[4]$ En effet, 11 et 7 ont le même reste dans la division euclidienne par 4.

Propriété :

Soient a, b et c des entiers relatifs et n entier naturel non nul.

- $a \equiv 0[n]$ si et seulement si a est divisible par n.
- $a \equiv a[n]$
- r est le reste de la division euclidienne de a par n si et seulement si $a \equiv r[n]$ avec la contrainte $0 \leq r < n$
- $a \equiv b[n]$ et $b \equiv c[n]$, alors $a \equiv c[n]$

b) *Calculer avec des congruences*

Propriété :

Soient a, b , c et d des entiers relatifs et n entier naturel non nul.

- Si $a \equiv b[n]$ alors $a + c \equiv b + c[n]$
- Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $a + c \equiv b + d[n]$. On dit que l'addition est compatible avec les congruences.
- Si $a \equiv b[n]$, alors Si $ac \equiv bc[n]$
- Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $ac \equiv bd[n]$; On dit que la multiplication est compatible avec les congruences.
- Si $a \equiv b[n]$ alors $a^p \equiv b^p[n]$ avec p un entier naturel non nul.

Attention :

La division n'est pas compatible avec les congruences.
En effet $5 \times 4 \equiv 5 \times 6[10]$ mais 4 et 6 ne sont pas congrus modulo 10.

Exercice 1 :

Résoudre les équations suivantes :

- $x + 3 \equiv 2[7]$
- $x^2 \equiv 0[4]$

Solutions :

- $x + 3 \equiv 2[7] \Leftrightarrow x \equiv -1[7] \Leftrightarrow x = -1 + 7k, k \in \mathbb{Z}$
- Pour résoudre $x^2 \equiv 0[4]$, on raisonne par disjonction de cas sur x.

Si $x \equiv$ ...[4]	0	1	2	3
Alors $x^2 \equiv \cdots [4]$	0	1	0	1

On a donc $x \equiv 0[4]$ et $x \equiv 2[4]$ qui conviennent.
Les solutions sont donc $x = 4k, k \in \mathbb{Z}$ et $x = 4k' + 2, k' \in \mathbb{Z}$

Exercice 2 :

Montrer que $2^{3n} - 1$ est un multiple de 7.

Solution :

On a $2^3 = 8$ soit $2^3 \equiv 1[7]$. Par compatibilité avec les puissances, on a : $(2^3)^n \equiv (1)^n[7]$
Soit donc $2^{3n} \equiv 1[7]$ et donc $2^{3n} - 1$ est un multiple de 7.

Exercice 3 :

Déterminer le reste de la division euclidienne de 11^{2020} par 3.

Solution :

On a $11 \equiv 2[3]$ puis que $11^2 \equiv 1[3]$. Ainsi, $\forall q > 0, 11^{2q} \equiv 1[3]$.
Or $2020 = 1010 \times 2$ donc $11^{2020} \equiv 1[3]$
Comme $0 \leq 1 < 3$, 1 est bien le reste de la division euclidienne de 11^{2020} par 3.