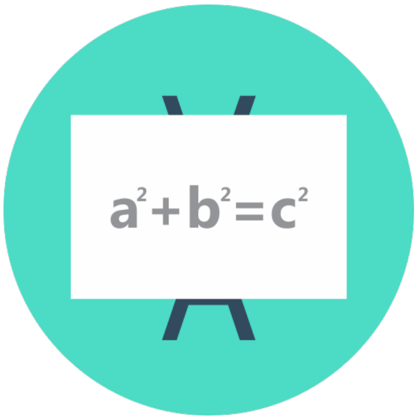

Chapitre XIII - Arithmétique (Spécialité)

Bacomathiques — https://bacomathiqu.es

TABLE DES MATIÈRES

I - Divisibilité et congruence

1. Divisibilité

Soient a et b deux entiers relatifs. On dit que a est divisible par b s'il existe un $k \in \mathbb{Z}$ tel que :

$$a = k \times b$$

Si on a bien b divise a, alors $-b$ divise a.

Soient a, b et c trois entiers relatifs avec $c \neq 0$:

Si c divise a et b, alors pour tout $u, v \in \mathbb{Z}$: c divise $u \times a + v \times b$.

On appelle **division euclidienne**, l'opération qui a deux entiers a (dividende) et $b \neq 0$ (diviseur) fait correspondre deux autres entiers q (quotient) et r (reste).

Ainsi, pour ces entiers relatifs a et b, il existe q et r entiers relatifs tels que :

$$a = b \times q + r \text{ avec } 0 \leq r \leq |b|$$

2. Les multiples

Soient a et b deux entiers relatifs avec $b \neq 0$, a est un multiple de b si et seulement si b est un diviseur de a. On a les propriétés suivantes :

- Si a est un multiple de b alors $-a$ est un multiple de b.
- La somme ainsi que la différence de certains multiples de b est un multiple de b.
- Si a est un multiple de b alors pour $k \in \mathbb{Z}$, $k \times a$ est un multiple de b.

3. Les congruences

Soient a, b et n trois entiers avec $n \geq 2$. a **est congru à** b **modulo** n (noté $a \equiv b[n]$) si et seulement si :

— $(a - b)$ est multiple de n.

— a et b ont le même reste dans la division euclidienne par n.

Ces deux formules précédentes sont équivalentes : si on a la congruence alors ces formules sont toutes deux valables et réciproquement.

Une propriété pouvant se dégager des congruences est que a est divisible par b si et seulement si $a \equiv 0[b]$.

Les opérations suivantes sont disponibles avec les congruences pour a, b, c et d quatre entiers relatifs :

— Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $a + c \equiv b + d[n]$.

— Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $a - c \equiv b - d[n]$.

— Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $a \times c \equiv b \times d[n]$.

— Si $a \equiv b[n]$ alors $a \times c \equiv b \times c[n]$.

— Si $a \equiv b[n]$ alors $a^k \equiv b^k[n]$ pour $k \in \mathbb{N}^*$.

Exemple : On donne $5^6 \equiv 1[7]$. Déterminez le reste de la division euclidienne de 2406^{2015} par 7.

Faisons la division euclidienne de 2406 par 7. On obtient le quotient $q = 343$ et le reste $r = 5$.
On a ainsi $2406 \equiv 5[7]$ ce qui implique que $2406^{2015} \equiv 5^{2015}[7]$.

Or d'après l'énonce, $5^6 \equiv 1[7]$. Faisons la division euclidienne de 2015 par 6 :
On obtient que $2015 = 6 \times 335 + 5$.

Ainsi, on a $2406^{2015} \equiv 5^{2015}[7]$
$\iff 2406^{2015} \equiv 5^{6\times 335+5}[7]$
$\iff 2406^{2015} \equiv (5^6)^{335} \times 5^5[7]$
$\iff 2406^{2015} \equiv (1)^{335} \times 5^5[7]$ (car $5^6 \equiv 1[7]$)
$\iff 2406^{2015} \equiv 5^5[7]$
Le reste de la division euclidienne de 2406^{2015} par 7 est donc $5^5 = 3125$.

II - PGCD et théorème de Bézout

1. Le PGCD

Le Plus Grand Commun Diviseur de deux nombres entiers relatifs a et b (avec a ou b non nul) noté $PGCD(a;b)$ est le plus grand entier qui les divise simultanément. Ainsi, on a les propriétés suivantes :

- $PGCD(a;1) = 1$
- $PGCD(a;0) = a$
- $PGCD(k \times a; k \times b) = k \times PGCD(a;b)$ pour $k \in \mathbb{N}^*$
- Si b divise a alors $PGCD(a;b) = |b|$

Il existe une manière de déterminer le PGCD de deux entiers naturels non nuls a et b avec $b < a$ appelée **Algorithme d'Euclide**. Pour obtenir $PGCD(a;b)$, on procède comme suit :

1. On fait la division euclidienne de a par b et on appelle r le reste.
2. Si $r = 0$, alors $PGCD(a;b) = b$.
3. Sinon on recommence l'étape 1 en remplaçant a par b et b par r.

On dit que deux nombres sont **premiers entre eux** si leur PGCD est égal à 1. Ainsi, soient $a, b \in \mathbb{N}^*$:

$$PGCD(a;b) = d \text{ si et seulement si } PGCD\left(\frac{a}{d};\frac{b}{d}\right) = 1.$$

2. Théorème de Gauss

Soient a, b et c trois entiers non nuls. Alors on a :

Si c divise ab et c premier avec a, alors c divise b.

3. Théorème de Bézout

Soient a et b deux entiers relatifs non nuls et d leur PGCD. Il existe deux entiers relatifs u et v tels que :

$$ua + vb = d$$

Une conséquence de ce théorème est que a et b sont premiers entre eux si et seulement s'il existe u et v tels que :

$$ua + vb = 1$$

Exemple : Calculez $PGCD(250; 150)$. En déduire u et v entiers relatifs non nuls tels que $50 = u \times 250 + v \times 150$. Calculons le PGCD de 250 et 150 par l'algorithme d'Euclide : Division euclidienne de 250 par 150 : $250 = 150 \times 1 + 100$.
Division euclidienne de 150 par 100 : $150 = 100 \times 1 + 50$.
Division euclidienne de 100 par 50 : $100 = 5 \times 2 + 0$.

On a $PGCD(250; 150) = 50$. Déterminons u et v :
$250 = 150 \times 1 + 100 \iff 150 = 1 \times 250 - 1 \times 100$
$150 = 1 \times 100 + 50 \iff 50 = 150 - 1 \times 100$
$\iff 50 = 1 \times 250 - 1 \times 100 - 1 \times 100 = 1 \times 250 - 2 \times 100$

On a par conséquent $u = 1$ et $v = -2$.

III - Les nombres premiers

1. Définition

Soit un entier naturel n :

> n est dit **premier** s'il n'admet que deux diviseurs distincts, entiers et positifs : 1 et lui-même.

> **Remarque :** L'ensemble des nombres premiers est infini.

2. Propriétés

Soit $n \in \mathbb{N}$ supérieur ou égal à 2, alors on a les propriétés suivantes :

> — Si n n'admet aucun diviseur premier inférieur ou égal à $\sqrt{n}$, alors n est premier.
> — Si n n'est pas premier alors n admet au moins un diviseur premier inférieur ou égal à $\sqrt{n}$.

Soient a un entier relatif et n un entier naturel. Alors :

> Si n est premier et n ne divise pas a, alors a et n sont premiers entre eux.

Soient a et b deux entiers relatifs et n un entier naturel. On a :

> — Si n est premier et divise ab alors n divise a ou n divise b.
> — Si a, b et n sont premiers et n divise ab alors $n = a$ ou $n = b$.

3. Décomposition de nombres

Soit $n \in \mathbb{N}$ supérieur ou égal à 2, alors n peut s'écrire de la façon suivante :

$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ \dots \ \times p_n^{\alpha_n}$
avec p_1, p_2, ... , p_n des nombres premiers tels que $p_1 < p_2 < \ \dots \ < p_n$ et α_1, α_2, ... , α_n des entiers relatifs.

On appelle cette écriture **décomposition en facteurs premiers**.

Exemple : Décomposition de 200 en produit de facteurs premiers.

$200 = 2 \times 100$ (2 est le plus petit nombre premier qui divise 200)
$100 = 2 \times 50$ (2 est le plus petit nombre premier qui divise 100)
$50 = 2 \times 25$ (2 est le plus petit nombre premier qui divise 50)
$25 = 5 \times 5$ (5 est le plus petit nombre premier qui divise 25)
$5 = 5 \times 1$ (5 est un nombre premier, c'est terminé)

On a donc $200 = 2 \times 100 = 2 \times (2 \times 50) = \dots = 2^3 \times 5^2$.