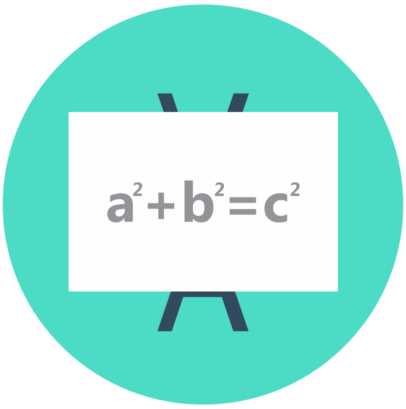


Chapitre XIV – Arithmétique (Maths expertes)

Bacomathiques — https://bacomathiqu.es

TABLE DES MATIÈRES

I - Divisibilité et congruence

1. Divisibilité

Dans toute la suite de cette section, on notera par $\mathbb{Z}$ l'ensemble des nombres entiers relatifs (i.e. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$) et par $\mathbb{N}$ l'ensemble des nombres entiers naturels (i.e. $\mathbb{N} = \{0, 1, 2, \dots\}$).

À RETENIR

Définition

Soient a et b deux entiers relatifs. On dit que b **divise** a (ou que a est **un multiple** de b) s'il existe $k \in \mathbb{Z}$ tel que $a = kb$. On note ceci par $b \mid a$.

À LIRE

Si on a b divise a, alors $-b$ divise a. Par exemple, comme 6 divise 12, alors -6 divise également 12.

À RETENIR

Propriétés

- Tout entier relatif b divise 0 (car $0 = 0 \times b$).
- 1 divise tout entier relatif a (car $a = a \times 1$).
- Si $c \mid a$ et $c \mid b$ alors $c \mid (au + bv)$ pour tout $u, v \in \mathbb{Z}$.

2. Division euclidienne

La **division euclidienne** est une notion mathématique que l'on aborde très tôt au cours de notre scolarité (dès la classe de CM1). Nous allons tenter de formaliser ceci :

À RETENIR

Théorème de la division euclidienne

Soient $a, b \in \mathbb{Z}$. On suppose $b \neq 0$. On appelle **division euclidienne** de a par b, l'opération qui à (a, b), associe le couple d'entiers relatifs (q, r) tel que $a = bq + r$ où $0 \leq r < |b|$. Un tel couple **existe** forcément et est **unique**.

À RETENIR

Vocabulaire

En reprenant les notations du théorème, a s'appelle le **dividende**, b le **diviseur**, q le **quotient** et r le **reste** de la division euclidienne.

À LIRE

Exemple

On souhaite effectuer la division euclidienne de 314 par 7. Posons-la :

$$\begin{array}{rrr|rr} 3 & 1 & 4 & 7 & \\ \cline{4-5} & 3 & 4 & 4 & 4 \\ & & 6 & & \end{array}$$

- On cherche combien de fois 7 est contenu dans 31 (cela ne sert à rien de commencer par 3 car $3 < 7$). On a $4 \times 7 = 28$ et $5 \times 7 = 35$ donc on écrit 4 sous le diviseur et le reste $31 - 28 = 3$. Puis, on abaisse le chiffre des unités qui est 4.
- On recommence : combien de fois 7 est-il contenu dans 34 ? Comme $4 \times 7 = 28$ et $5 \times 7 = 35$, 7 est contenu 4 fois dans 34 et il reste $34 - 28 = 6$.
- Comme $6 < 7$, la division euclidienne est terminée : on a $314 = 7 \times 44 + 6$.

Donnons enfin une propriété qui nous sera utile dans la section suivante.

À RETENIR

Propriété

Soit $n \in \mathbb{N}$ tel que $n \neq 0$. Deux entiers relatifs a et b ont le même reste dans la division euclidienne par n si et seulement si $a - b$ est un multiple de n.

3. Congruences dans $\mathbb{Z}$

À RETENIR

Définition

On dit que deux entiers relatifs a et b sont **congrus modulo** n (où n est un entier naturel supérieur ou égal à 2) si a et b ont le même reste dans la division euclidienne par n. On note alors $a \equiv b \mod n$.

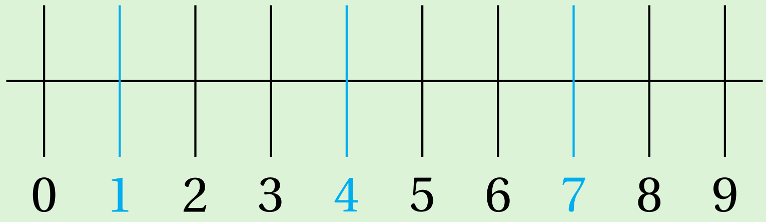
À LIRE

On remarque que a est un multiple de n si et seulement si $a \equiv 0 \mod n$.

À LIRE

Exemple

Par exemple, $1 \equiv 4 \equiv 7 \mod 3$.



On signale que la congruence est une **relation d'équivalence**.

À RETENIR

Propriétés

Soit $n \geq 2$. Pour tout $a, b, c \in \mathbb{Z}$:

- $a \equiv a \mod n$ (**réflexivité**)
- Si $a \equiv b \mod n$, alors $b \equiv a \mod n$ (**symétrie**)
- Si $a \equiv b \mod n$, et si $b \equiv c \mod n$, alors $a \equiv c \mod n$ (**transitivité**)

De plus, la congruence est compatible avec les opérations usuelles sur les entiers relatifs.

À RETENIR

Propriétés

Soit $n \geq 2$. Soient a, b, c et $d \in \mathbb{Z}$ tels que $a \equiv b \mod n$ et $c \equiv d \mod n$. Alors on a la compatibilité avec :

- L'**addition** : $a + c \equiv b + d \mod n$.
- La **multiplication** : $ac \equiv bd \mod n$.
- Les **puissances** : pour tout $k \in \mathbb{N}$, $a^k \equiv b^k \mod n$.

À LIRE

Exemple

Comme $7 \equiv 3 \mod 4$, et $5 \equiv 1 \mod 4$, on a $35 = 5 \times 7 \equiv 1 \times 5 \mod 4$.

II - PGCD et théorème de Bézout

1. Plus Grand Commun Diviseur

À RETENIR

Définition

Soient a, $b \in \mathbb{Z}$ non tous nuls. Le **Plus Grand Commun Diviseur** de a et b (noté $\text{PGCD}(a;b)$) est le plus grand entier positif qui les divise simultanément.

Avec cette définition, on peut dégager quelques propriétés.

À RETENIR

Propriétés

Soient a, $b \in \mathbb{Z}$ non tous nuls.

- $\text{PGCD}(a;b) = \text{PGCD}(b;a)$
- $\text{PGCD}(a;1) = 1$
- $\text{PGCD}(a;0) = a$
- Pour tout $k \in \mathbb{N}$, $\text{PGCD}(ka;kb) = k\,\text{PGCD}(a;b)$
- Si $b \mid a$, alors $\text{PGCD}(a;b) = |b|$

Il existe une manière de déterminer le PGCD de deux entiers naturels non nuls a et b avec $b < a$ appelée **Algorithme d'Euclide**.

À RETENIR

Algorithme d'Euclide

Soient a, $b \in \mathbb{Z}$ non tous nuls. Pour obtenir $\text{PGCD}(a;b)$, 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 $\text{PGCD}(a;b) = b$.
3. Sinon on recommence l'étape 1 en remplaçant a par b et b par r.

Terminons cette section par une définition.

À RETENIR

Nombres premiers entre eux

On dit que deux nombres sont **premiers entre eux** si leur PGCD est égal à 1.

À LIRE

Petite remarque : si on note d le PGCD de deux nombres a et b, alors $\frac{a}{d}$ et $\frac{b}{d}$ sont deux nombres premiers entre eux.

2. Théorème de Bézout

Un résultat fondamental de l'arithmétique est le **théorème de Bachet-Bézout** (que l'on rencontre parfois sous le nom d'**identité de Bézout**).

À RETENIR

Théorème de Bachet-Bézout

Soient a et b deux entiers relatifs non nuls. On note d leur PGCD. Alors il existe deux entiers relatifs u et v tels que $ua + vb = d$.

À RETENIR

Théorème de Bézout

Une conséquence de ce théorème est que a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs u et v tels que $ua + vb = 1$.

À LIRE

Exemple

Calculons PGCD$(250;150)$ et déduisons-en deux entiers relatifs u et v tels que $50 = 250u + 150v$. Commençons par calculer le PGCD de 250 et 150 par l'algorithme d'Euclide :

La division euclidienne de 250 par 150 donne $250 = 150 \times 1 + 100$.
La division euclidienne de 150 par 100 donne $150 = 100 \times 1 + 50$.
La division euclidienne de 100 par 50 donne $100 = 5 \times 2 + 0$.

On a PGCD$(250;150) = 50$. Déterminons u et v :

$250 = 150 \times 1 + 100 \iff 150 = 1 \times 250 - 1 \times 100$
$150 = 1 \times 100 + 50 \iff 50 = 150 - 1 \times 100$

Donc $50 = 1 \times 250 - 1 \times 100 - 1 \times 100 = 1 \times 250 - 2 \times 100$.

On a par conséquent $u = 1$ et $v = -2$. L'algorithme que l'on vient d'utiliser pour trouver u et v s'appelle l'**algorithme d'Euclide étendu**.

À RETENIR

Résolution d'une congruence simple

Supposons que l'on souhaite résoudre une congruence du type $ax \equiv b \mod n$ d'inconnue x. On pose $d = \mathrm{PGCD(a;n)}$. Alors :

1. Si d ne divise pas b, on cherche deux entiers u et v tels que $au + nv = 1$ (avec l'algorithme d'Euclide étendu par exemple). Les solutions de la congruence sont alors les entiers x vérifiant $x \equiv ub \mod n$.
2. Si $d \mid b$, cela revient à résoudre la congruence $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{n}{d}$, et on se ramène au cas 1 (avec la nouvelle congruence à résoudre).

À LIRE

Exemple

On souhaite résoudre la congruence $6x \equiv 6 \mod 9$. Alors, comme $d = \text{PGCD}(6;9) = 3$, on a $d \mid 6$. On se ramène donc à résoudre $2x \equiv 2 \mod 3$ (où 2 et 3 sont premiers entre eux).

On écrit l'identité de Bézout appliquée à 2 et 3 : $2 \times 2 + 3 \times -1 = 1$. Donc les solutions à la congruence du début sont les entiers x vérifiant $x \equiv 4 \mod 3 \equiv 1 \mod 3$ (i.e. les x de la forme $x = 3k + 1$ où $k \in \mathbb{Z}$).

3. Lemme de Gauss

À RETENIR

Lemme de Gauss

Soient a, b et c trois entiers non nuls. Si $c \mid ab$ et c est premier avec a, alors $c \mid b$.

À RETENIR

Corollaire

Soient a, b et c trois entiers non nuls. Si $b \mid a$, $c \mid a$ et que b et c sont premiers entre eux, alors $bc \mid a$.

4. Équations diophantiennes

À RETENIR

Définition

Une **équation diophantienne linéaire en deux variables** x et y est une équation de la forme (E) : $ax + by = c$ où les coefficients a, b et c sont des entiers relatifs et où les solutions sont également des entiers relatifs.

À RETENIR

Solutions de (E)

En reprenant les notations précédentes, on pose $d = \text{PGCD}(a;b)$. Alors :

— Si $d \mid c$, on cherche une solution particulière à (E) que l'on note $(x_0;y_0)$. Alors les solutions de (E) sont les couples $(x_k;y_k)$ où $x_k = x_0 + k\frac{b}{d}$ et $y_k = y_0 - k\frac{a}{d}$.

— Sinon, (E) n'a pas de solution.

À LIRE

Exemple

On cherche à résoudre l'équation diophantienne $(E) : 25x + 10y = 15$. Commençons par chercher une solution particulière $(x_0; y_0)$.

Comme $d = \text{PGCD}(25; 10) = 5$, on a $d \mid 15$. En divisant les deux côtés de l'égalité par 5, on a $(E) \iff 5x + 2y = 3$.

Cherchons une solution particulière à (E). On écrit l'identité de Bézout appliquée à 5 et 2 : $5 \times 1 + 2 \times -2 = 1$. Ainsi, en multipliant les deux côtés de l'égalité par 3, on obtient : $5 \times 3 + 2 \times -6 = 3$.

On a trouvé une solution particulière à (E) qui est le couple $(x_0; y_0)$ où $x_0 = 3$ et $y_0 = -6$. On pourrait appliquer la formule pour donner la forme générale des solutions de (E), mais essayons de ne pas l'utiliser.

Soit $(x; y)$ une autre solution de (E). On a $3 = 5x + 2y = 5x_0 + 2y_0$. D'où $5(x - x_0) = 2(y_0 - y)$ (en passant les x et x_0 du même côté de l'égalité et en faisant de même pour y et y_0, puis en factorisant).

Ainsi, on a $5 \mid 2(y_0 - y)$. Or, 5 et 2 sont premiers entre eux, donc par le lemme de Gauss, $5 \mid y_0 - y$. Il existe donc q_1 tel que $5q_1 = y_0 - y$, d'où $y = y_0 - 5q_1$.

De même, $2 \mid 5(x - x_0)$ avec 2 et 5 premiers entre eux, donc par le lemme de Gauss, $2 \mid x - x_0$. Il existe donc q_2 tel que $2q_2 = x - x_0$, d'où $x = x_0 + 2q_2$.

En réinjectant tout ça dans (E), on obtient $5(x_0 + 2q_2) + 2(y_0 + -5q_1) = 3 \iff \underbrace{5x_0 + 2y_0}_{=3} + 10q_2 - 10q_1 = 3 \iff q_1 = q_2$.

Les solutions de (E) sont donc les couples $(x_k; y_k)$ où $x_k = x_0 + 2k$ et $y_k = y_0 - 5k$ (et on a bien les mêmes résultats qu'avec la formule).

III - Nombres premiers

1. Définition

Commençons cette section par définir ce qu'est un **nombre premier**. Il s'agit là d'une notion dont entend parler très tôt au cours de notre scolarité, sans pour autant vraiment rentrer dans le sujet. Détaillons donc un peu tout ceci.

À RETENIR

Nombre premier

Un nombre entier $p \geq 2$ est dit **premier** si ses seuls diviseurs positifs sont 1 et lui-même.

À LIRE

Exemple

2, 3, 5, 7, 11 et 13 sont des nombres premiers.

2. Propriétés

Voici quelques propriétés basiques que possèdent les nombres premiers.

À RETENIR

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 $\sqrt{n}$.
- Si n est premier et n ne divise pas un entier m, alors n et m sont premiers entre eux.

À RETENIR

Lemme d'Euclide

Soit p un nombre premier et a et b deux entiers. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

On donne enfin un résultat fondamental (mais qui reste très simple) sur l'ensemble des nombres premiers.

À RETENIR

Infinité de nombres premiers

Il existe une infinité de nombres premiers.

DÉMONSTRATION

Infinité de nombres premiers

Supposons par l'absurde que l'ensemble des nombres premiers soit un ensemble fini. On note par P cet ensemble et par r sont cardinal. On a donc $P = \{p_1, p_2, \dots, p_r\}$ où p_1, p_2, ... , p_r sont premiers.

Soit $N = p_1 \times p_2 \times \cdots \times p_r + 1$. Alors, $N \notin P$ donc N n'est pas premier (et est strictement supérieur à 1). Il existe donc un nombre premier qui divise N.

En d'autres mots, il existe $i \in \{1, \dots, r\}$ tel que $p_i \mid N$. De plus, $p_i \mid p_1 \times p_2 \times \cdots \times p_r$.

Donc $p_i \mid N - p_1 \times p_2 \times \cdots \times p_r \iff p_i \mid 1$, donc $p_i = 1$ ou $p_i = 0$: c'est absurde car $p_i \geq 2$.

Pour la petite histoire, c'est Euclide qui a fourni une première version de cette preuve en 300 av. J.-C!

À RETENIR

Petit théorème de Fermat

Soit p un nombre premier et a un entier non divisible par p. Alors $a^{p-1} \equiv 1 \mod p$.

À LIRE

Cela revient au même de dire que si a est un entier quelconque et que p est un nombre premier, alors $a^p \equiv a \mod p$.

3. Décomposition de nombres

Passons maintenant à un résultat fondamental de l'arithmétique : le principe de **décomposition en produit de facteurs premiers** (il s'agit même là d'un théorème qui est sobrement intitulé **théorème fondamental de l'arithmétique**).

À RETENIR

Théorème fondamental de l'arithmétique

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

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n}$$

où p_1, p_2, ... , p_n des nombres premiers tels que $p_1 < p_2 < \cdots < p_n$ et α_1, α_2, ... , α_n des entiers naturels non nuls.

À LIRE

Exemple

Décomposons 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 $200 = 2 \times 100 = 2 \times (2 \times 50) = \cdots = 2^3 \times 5^2$.