CHAP 04 Rappels d'arithmétique

Compétences

- Effectuer une division euclidienne et interpréter le quotient et le reste
- Utiliser les critères de divisibilité et le test de primalité
- Décomposer un entier en produit de facteurs premiers
- Calculer et utiliser un PGCD
- Utiliser les congruences : réduire modulo n, utiliser les compatibilités
- Résoudre un problème en situation (cycles, codage, cryptage)



Fil rouge *coloration drone*

Les communications entre un drone et sa station au sol sont souvent **chiffrées** : les nombres premiers et les congruences sont au cœur de ces méthodes.
Les congruences servent aussi à gérer les **cycles** (maintenance tous les n jours, rotation des équipes), et le PGCD à répartir du matériel en **lots identiques**.



I. Diviseurs, multiples, nombres premiers

I.1. Diviseurs et multiples

Définition 1.1

On dit que a est un **diviseur** de b ou que b est un **multiple** de a s'il existe un entier k tel que $b = k \times a$.
On dit aussi que b est **divisible** par a.

Propriété 1.1

On a les résultats suivants :

Un entier naturel est divisible par :	Si :
2	son chiffre des unités est 0 ou 2 ou 4 ou 6 ou 8
3	la somme de ses chiffres est divisible par 3
4	le nombre formé des deux derniers chiffres est divisible par 4
5	son chiffre des unités est 0 ou 5
9	la somme de ses chiffres est divisible par 9
10	son chiffre des unités est 0
11	la somme alternée de ses chiffres est divisible par 11

I.2. Nombres premiers

Définitions 1.2

Un entier naturel p est **premier** s'il admet exactement deux diviseurs : 1 et lui-même.

Propriété 1.2 *(Test de primalité)*

Si un entier n'admet aucun diviseur premier inférieur ou égal à sa racine carrée, alors il est premier.

Théorème 1.1

Tout entier naturel strictement supérieur à 1 peut être écrit comme un produit de nombres premiers de façon unique, à l'ordre près des facteurs. On appelle ce produit la « décomposition en facteurs premiers ».

Méthode 1.1

Pour trouver le **nombre** de diviseurs d'un entier N à partir de sa décomposition en facteurs premiers, on multiplie les exposants, augmentés de 1, des facteurs premiers apparaissant dans la décomposition de N.

Licence Ouverte Etalab 2.0

▸ **Méthode 1.2**

Pour déterminer la liste de tous les diviseurs d'un entier N, on utilise un **arbre** (de type *multiplicatif*).
Cet arbre permet également de retrouver le nombre de diviseurs de l'entier N.

II. Division euclidienne, congruences

II.1. Division euclidienne

▸ **Définition 2.1**

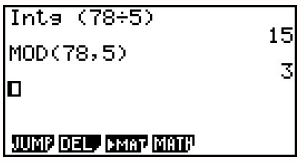
a et b étant deux entiers relatifs tels que $b \neq 0$, il existe un unique couple $(q\,;r)$ d'entiers relatifs tel que :

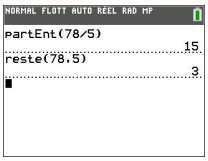
$$\begin{cases} a = b \times q + r \\ 0 \leqslant r < |b| \end{cases}.$$

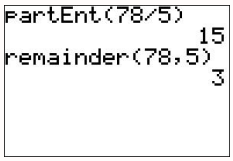
L'entier q est le quotient et l'entier r est le reste de cette division.

▸ **Méthode 2.1** *(Calculatrice)*

La partie entière donne le quotient de la division euclidienne de a par b.
La fonction CASIO `MOD` ou TEXAS `reste` ou TEXAS `remainder` donne le reste de la division euclidienne de a par b :







▸ **Propriétés 2.1**

b divise a si et seulement si le reste de la division euclidienne de a par b est égal à 0.

II.2. Congruences

▸ **Définition 2.2**

Soit n un entier supérieur ou égal à 2, et soient a et b deux entiers quelconques de $\mathbb{Z}$.
On dit que a et b sont **congrus** modulo n si et seulement si $a - b$ est un multiple de n, c'est-à-dire s'il existe un entier relatif k tel que $a - b = kn$.

▸ **Notation 2.1**

Cela se note $a \equiv b \ [n]$ et on lit : « a est congru à b modulo n ».

▸ **Définition 2.3**

Soit n un entier supérieur ou égal à 2, et soient a et b deux entiers quelconques de $\mathbb{Z}$.
On dit que a et b sont congrus modulo n si et seulement si a et b ont le même reste dans la division par n.

▸ **Conséquences 2.1**

- $a \equiv 0 \ [n] \Leftrightarrow a$ est un multiple de n.
- Si $a = nq + r$ avec $0 \leqslant r < n$ alors $a \equiv r \ [n]$.
- Si $a \equiv r \ [n]$ avec $0 \leqslant r < n$ alors r est le reste dans la division de a par n.

r est le plus petit entier positif congru à a modulo n.

▸ **Propriétés 2.2**

- Si $a \equiv b \ [n]$ et $b \equiv c \ [n]$ alors $a \equiv c \ [n]$.
- Si $a \equiv b \ [n]$ alors $a + c \equiv b + c \ [n]$ et $ac \equiv bc \ [n]$.

Licence Ouverte Etalab 2.0

▸ **Théorème 2.1**

Si a, a', b, b' sont des entiers tels que $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$ alors :

- $a + b \equiv a' + b' \ [n]$ et $a - b \equiv a' - b' \ [n]$;
- $a \times b \equiv a' \times b' \ [n]$;
- $k \times a' \equiv k \times a \ [n]$ avec k un entier ;
- $a^k \equiv (a')^k \ [n]$ avec k un entier naturel.

▸ **Calculatrice 2.1**

On peut travailler sur les congruences en utilisant le reste de la div. eucl. (via `reste`/`remainder`/`MOD`).

III. PGCD

III.1. Définitions

▸ **Définition 3.1**

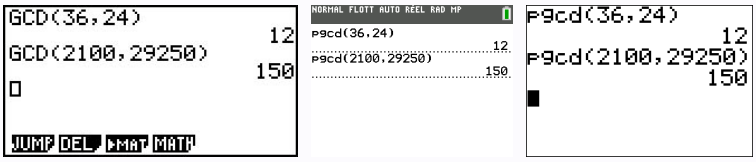
Le PGCD des deux entiers a et b, noté PGCD(a ; b) est le plus grand des diviseurs communs à a et à b.

▸ **Méthode 3.1**

Pour calculer PGCD(a ; b) :

- on écrit la décomposition en facteurs premiers de a et de b ;
- on multiplie entre eux les facteurs premiers communs aux deux décompositions, affectés du plus petit exposant figurant dans ces décompositions.

▸ **Calculatrice 3.1**



▸ **Définition/Propriétés 3.2**

a et b sont dits premiers entre eux lorsque leur seul diviseur commun est 1.

a et b sont premiers entre eux si et seulement si leur PGCD est égal à 1.
Deux nombres premiers distincts sont premiers entre eux.

III.2. Algorithme d'Euclide

▸ **Méthode 3.2**

Pour calculer PGCD(a ; b) où $a > b$:

- on effectue la division euclidienne de a par b : on obtient un reste r avec $r < b$:
  - si $r = 0$, alors a est divisible par b et PGCD(a ; b) = b ;
  - si $r \neq 0$, alors PGCD(a ; b) = PGCD(b ; r) ;
- on effectue la division euclidienne de b par r : on obtient un nouveau reste r_1 avec $r_1 < r$:
  - si $r_1 = 0$ alors b est divisible par r et PGCD(a ; b) = PGCD(b ; r) = r ;
  - si $r_1 \neq 0$ alors on réitère le processus avec r et r_1 ;
- on s'arrête lorsque l'on trouve un reste égal à 0 ; le PGCD(a ; b) est alors le dernier reste non nul obtenu.

Licence Ouverte Etalab 2.0