Algorithmes d'Arithmétique

1. Définition et Enjeux

Les **algorithmes d'arithmétique** regroupent l'ensemble des méthodes, logiques et traitements appliqués aux nombres entiers. Ils sont fondamentaux en programmation pour résoudre des problèmes mathématiques liés à la divisibilité, aux nombres premiers, ou au calcul du PGCD et du PPCM.

Ces algorithmes ne sont pas de simples exercices théoriques. Ils constituent la base de domaines critiques de l'informatique moderne, notamment la **cryptographie** (comme le chiffrement RSA qui sécurise les transactions sur Internet, basé sur les nombres premiers géants), la compression de données et l'optimisation des calculs.

2. L'outil fondamental : L'opérateur Modulo

Pour faire de l'arithmétique en programmation, l'outil le plus puissant est l'opérateur **Modulo** (souvent représenté par le symbole `%` ou le mot-clé `MOD`). Le modulo renvoie le **reste de la division euclidienne** d'un entier par un autre.

- Si `A modulo B = 0`, cela signifie que le reste de la division est nul. Donc, **A est divisible par B** (ou B est un diviseur de A).
- **Exemple :** `10 % 2 = 0` (10 est pair). `10 % 3 = 1` (10 n'est pas divisible par 3).

3. Les Nombres Premiers

Un entier naturel (supérieur ou égal à 2) est dit **premier** s'il n'admet que deux diviseurs distincts : 1 et lui-même (exemples : 2, 3, 5, 7, 11...).

Pour vérifier si un nombre `N` est premier, l'algorithme naïf consiste à tester sa divisibilité par tous les entiers compris entre 2 et `N-1`. Cependant, pour des raisons d'optimisation, il suffit mathématiquement de tester les diviseurs jusqu'à la **racine carrée de N**. Si aucun diviseur n'est trouvé jusque-là, le nombre est premier.

Algorithme optimisé (Pseudo-code) :

```
Fonction EstPremier(N : Entier) : Booléen
Variables
    i : Entier
```

```
Début
    Si N < 2 Alors
        Retourner Faux
    FinSi

    // On teste les diviseurs de 2 jusqu'à la racine carrée de N
    Pour i allant de 2 à Racine(N) Faire
        Si N modulo i = 0 Alors
            Retourner Faux // On a trouvé un diviseur, il n'est pas premier
        FinSi
        i <- i + 1
    FinPour

    Retourner Vrai
Fin
```

4. Le PGCD et l'Algorithme d'Euclide

Le **PGCD** (Plus Grand Commun Diviseur) de deux nombres entiers non nuls est le plus grand entier qui divise simultanément ces deux nombres.

L'**algorithme d'Euclide** est l'une des méthodes les plus anciennes et les plus élégantes pour calculer le PGCD de deux nombres (A et B). Le principe est basé sur des divisions successives : on remplace A par B, et B par le reste de la division de A par B, jusqu'à ce que le reste soit égal à zéro. Le PGCD est alors **le dernier reste non nul**.

Algorithme d'Euclide (Version Itérative) :

```
Fonction PGCD(A : Entier, B : Entier) : Entier
Variables
    Reste : Entier
Début
    Tant Que B ≠ 0 Faire
        Reste <- A modulo B
        A <- B
        B <- Reste
    FinTantQue

    Retourner A
Fin
```

apcpedagogie.com

5. Le PPCM (Plus Petit Commun Multiple)

Le **PPCM** de deux entiers est le plus petit entier positif qui est multiple à la fois de l'un et de l'autre. En programmation, on utilise très rarement une boucle pour trouver le PPCM, car il existe une relation mathématique directe et très rapide avec le PGCD :

Formule : `PPCM(A, B) = | A * B | / PGCD(A, B)`

Algorithme du PPCM :

```
Fonction PPCM(A : Entier, B : Entier) : Entier
Début
    Si A = 0 Ou B = 0 Alors
        Retourner 0
    Sinon
        Retourner (ValeurAbsolue(A * B) / PGCD(A, B))
    FinSi
Fin
```

6. Outil Interactif : Visualiser l'Algorithme d'Euclide

Pour bien comprendre comment fonctionne le calcul du PGCD et du PPCM en machine, utilisez le simulateur ci-dessous. Entrez deux nombres et observez les divisions successives étape par étape jusqu'à l'obtention du résultat.

Rédigé et structuré par : **Med Khalil Kribi**

Source : https://apcpedagogie.com/algorithmes-arithmetique · téléchargé le 07/11/2026 · © APC Pédagogie · apcpedagogie.com