Le Théorème Fondamental de l'Arithmétique

Pierre VARNIER
Antoine GRENIER

18 janvier 2025

Contents

1 Introduction **2**

2 Notation et définition **2**
- 2.1 Définition nombre premier 2
- 2.2 Théorème fondamental de l'arithmétique 3
- 2.3 Preuve 3
- 2.4 Exemple d'une décomposition 3

3 Algorithmes **4**
- 3.1 Algorithme de décomposition 4
- 3.2 Algorithme de PGCD 4
- 3.3 Algorithme de PPCM 4

4 Image **5**

5 Référence **5**

1 Introduction

Je ne peux pas faire de dépot sur git isima.

Le théorème fondamental de l'arithmétique prouve que tout entier supérieur ou égal à 2 possède une décomposition unique en facteurs de nombres premiers.

2 Notation et définition

Notons $\mathbb{N}$ l'ensemble des entiers naturels

Exemple : 1. $Desentiersnaturelssontparexemples 0, 1, 2...$

2.1 Définition nombre premier

Définition : 1. *Nombres Premiers*
Un nombre premier est un nombre qui ne peut être divisé que par lui-même et par 1.

Exemple : 2. $Desexemplesdenombrespremierssont 2, 3, 5, 7...$

Définition : 2. *Le PGCD (Plus Grand Dénominateur Commun)*
Le PGCD de 2 nombres est le plus grand entier naturel qui divise simultanément ces 2 nombres.

Exemple : 3. $PGCD(24; 36) = 12$

Grâce au PGCD, on peut donc trouver les diviseurs communs de 24 *et* 36*, qui sont les diviseurs de* 12 *:* $1; 2; 3; 4; 6; 12$

Définition : 3. *Le PPCM (Plus Petit Multiple Commun)*
Le PPCM de 2 nombres est le plus petit entier strictement positif qui soit multiple de ces deux nombres.

Exemple : 4. $PPCM(16; 24) = 48$
$16 \times 3 = 48$
$24 \times 2 = 48$

2.2 Théorème fondamental de l'arithmétique

Théorème : 1. *Tout entier naturel* $\mathbb{N} \geq 2$ *peut être écrit de manière unique (à l'ordre des facteurs près) comme un produit de nombres premiers.*

2.3 Preuve

On va d'abord démontrer l'existence d'une décomposition, puis son unicité.

2.3.1 Existence

Lemme : 1. *Pour démontrer l'existence, on peut utiliser une recurrence :*

- *Initialisation : Pour n=2, qui est un nombre premier, la décomposition est lui même soit 2.*
- *Recurrence :*
  - *Hypothèse : Supposons que* $\forall k \in \mathbb{N} \in [2; n]$*, on peut l'écrire comme un produit de nombres premiers.*
  - *Recurrence : On veut montrer que* $n + 1$ *peut aussi être écrit comme un produit de nombre premiers :*
  - *1. Si* $n+1$ *est un nombre premier, alors il est déjà une décomposition en produit de nombres premiers, avec un seule facteur.*
  - *2. Si* $n + 1$ *n'est pas premier, alors il existe 2 entiers* a *et* b *tels que* $n + 1 = a * b$*, avec* $2 \leq a \leq b < n + 1$*. Par hypothèse de recurrence,* a *et* b *peuvent être décomposés en produits de nombres premiers. En multipliant ces décompositions, on obtient alors une décomposition de* $n + 1$
- *Conclusion : On a donc* $\forall n \in \mathbb{N}, n > 1$*, qui peut être écrit comme un produit de nombres premiers.*

2.3.2 Unicité

Lemme : 2. *La preuve de l'unicité peut être obtenue à partir du lemme d'Euclide selon lequel, si un nombre premier* p *divise un produit* ab*, alors il divise* a *ou il divise* b*. Maintenant, prenons deux produits de nombres premiers qui sont égaux. Prenons n'importe quel nombre premier* p *du premier produit.*

2.4 Exemple d'une décomposition

Exemple : 5. 60 *peut se décomposer comme :*

- $60 = 2 \times 30$
- $60 = 2 \times 2 \times 15$
- $60 = 2^2 \times 3 \times 5$
  C'est la décomposition unique.

3 Algorithmes

3.1 Algorithme de décomposition

Algorithme de décomposition

1. Entrer un entier $n \geq 2$
2. implémenter un i qui va de 2 à $\sqrt{n}$
3. Verifier n modulo $i == 0$
   (a) si n% i == 0
   i sera un des facteurs premiers de n
   n prendra la valeur de $\frac{n}{i}$ i prendra la valeur 2

   (b) sinon
   i prendra la valeur de $i + 1$
   (c) si $i > sqrtn$:
   n est un nombre premier et fera partie de la factorisation. n prendra la valeur de $\frac{n}{n} = 1$
4. On reproduit les étapes précédentes jusqu'à avoir $n = 1$

3.2 Algorithme de PGCD

Algorithme de PGCD

1. On peut réutiliser l'algorithme de décomposition précédent sur 2 nombres a et b.
2. On compare les valeurs de chacune des 2 décompositions.
   (a) Si il y a des valeurs en communs :
   On gardera la plus grande valeur commune.

   (b) sinon
   $PGCD(a; b) = 1$

3.3 Algorithme de PPCM

Algorithme de PPCM

1. Entrer 2 nombres a et b.
2. Implémenter un i dont les valeurs vont de 2 à b et un j dont les valeurs vont de 2 à a.
3. On compare chaque valeur de $b \times j$ et $a \times i$
4. On garde les valeurs communes et on retiens la plus petite c'est le PPCM.

4 Image

Voici une image d'écran4.
beginfigure[hbtp]
captionCapture
centering
includegraphics[scale=1].../../../../tmp/Captures d'écran/Capture d'écran du 2024-12-03
endfigure

5 Référence

- Page Wikipédia sur la décomposition en produit de facteurs premiers.