1 Décomposition en facteurs premiers

Définition 1 *Tout entier naturel $p \geqslant 2$ est dit premier s'il n'a que deux diviseurs 1 et lui-même*

Exemples : 2, 3, 5 sont premiers, 6 ne l'est pas car $6 = 2 \times 3$

Lemme 1 *Tout entier naturel $n \geqslant 2$ est divisible par un nombre premier*

Preuve

Dans beaucoup de démonstrations mathématiques on se base sur le caractère ***extrémal*** *d'un objet pour aboutir à une contradiction*

$\mathcal{D}(n)^*$ l'ensemble des diviseurs de n privé de 1, est une partie non vide de $\mathbb{N}$ donc il existe un plus petit élément p de $\mathcal{D}(n)^*$. Montrons que p est premier

Supposons le contraire, autrement dit $p = \min(\mathcal{D}(n)^*)$ est divisible par a entier naturel tel que $1 < a < p$, donc $a|n$ et $a < p$ donc p n'est pas le plus petit des diviseurs de n différents de 1, d'où la contradiction

Théorème 1 *L'ensemble des nombres premiers est* ***infini*** *:*

Preuve

Supposons le contraire , c'est à dire supposons que l'ensemble des nombres premiers est une suite **finie**, composé des nombres $\{ p_1 = 2, p_2 = 3, ..., p_n \}$

Montrons maintenant que le nombre $N = p_1...p_n + 1$ est premier et puisqu'il n' est pas dans la liste précédente puisqu'il est strictement plus grand que les nombres de la liste, on aboutit à une contradiction

N n' est divisible par aucun des p_i car $N \equiv 1\ [p_i]$ pour tout i

Or d'après le lemme 1 N est divisible par un nombre premier d'où la contradiction

Théorème 2 *Tout entier naturel supérieur ou égal à 2 se décompose de manière unique en un produit de nombres premiers*

Preuve

Existence

Par récurrence (forte) sur n

(Initialisation) Vrai pour les nombres premiers

(Hérédité) Supposons que la propriété est vraie pour $2 \leqslant k < n$

Si n est premier alors il n' y a rien à faire sinon d'après le lemme 1 il existe deux entiers q avec $p \geqslant 2$ **premier** plus petits que n tel que $n = qp$, en appliquant l'hypothèse de récurrence sur q , n à son tour se décompose en produit de nombres premiers

Unicité

Par récurrence (forte) sur n

(Initialisation) Vrai pour les nombres premiers

(Hérédité) Supposons que la propriété est vraie pour $2 \leqslant k < n$

On sait que $n = \prod_i p_i^{\alpha_i}$ (Existence)

pour pouvoir utiliser l'hypothèse de récurrence divisons n par $p_0^{\alpha_0}$ (on a choisi un des nombres premiers dans la décomposition)

Par conséquent $n = p_0^{\alpha_0} \times A$ et p_0 n'est pas dans la décomposition de A

Or $A < n$ donc par hypothèse de récurrence $A = \prod_i p_i^{\alpha_i}$ avec $p_i \neq p_0$ et les p_i sont uniques à l'ordre près

Est il possible que $p_0^{\alpha_0} A = p_1^{\alpha_1} A$ avec p_0 et p_1 premiers différents ?

Non car p_0 divise $p_1^{\alpha_1} A$ et est premier avec A d'après **le lemme de Gauss** p_0 divise $p_1^{\alpha_1}$ ce qui est absurde

D'où l'unicité

Définition 2 *Etant donné deux entiers supérieurs ou égaux à 1 ,n et m, on peut parler du plus petit commun multiple de n et m noté ppcm*$(m; n)$

En effet l'ensemble des multiples communs à m et n, $\mathcal{M}(m, n)$ *est une partie non vide de* $\mathbb{N}$ *car il contient le produit nm*

Théorème 3 $pgcd(\prod_i p_i^{\alpha_i} \ , \ \prod_i p_i^{\beta_i}) = \prod_i p_i^{\min(\alpha_i, \beta_i)}$

$ppcm(\prod_i p_i^{\alpha_i} \ , \ \prod_i q_i^{\beta_i}) = \prod_i p_i^{\max(\alpha_i, \beta_i)}$

Preuve

1. $\prod_i p_i^{\gamma_i}$ est un diviseur commun à m et à n si et seulement si $\gamma_i \leqslant \alpha_i$ et $\gamma_i \leqslant \beta_i$
   (Avec cette écriture si p_i n'est pas un facteur premier de m par exemple alors l'exposant $\alpha_i = 0$)
   D'où le résultat pour le pgcd
2. $\prod_i p_i^{\gamma_i}$ est un multiple commun à m et à n si et seulement si $\gamma_i \geqslant \alpha_i$ et $\gamma_i \geqslant \beta_i$
   d'où le résultat pour le ppcm

Exemple : $84 = 2^2 \times 3 \times 7$ et $70 = 2 \times 5 \times 7$

Pour le pgcd on prend les facteurs premiers communs avec leur exposant au minimum ainsi pgcd(84,70) $= 2 \times 7 = 14$

Pour le ppcm on prend tous les facteurs premiers avec leur exposant au maximum ainsi ppcm(42,70) $= 2^2 \times 3 \times 5 \times 7 = 420$

Théorème 4 $pgcd(n \ , \ m) \times ppcm(n \ , \ m) = nm$

Preuve

$\prod_i p_i^{\alpha_i} \prod_i p_i^{\beta_i} = \prod_i p_i^{\alpha_i + \beta_i}$

Or $\alpha_i + \beta_i = \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i)$

Donc $\prod_i p_i^{\alpha_i + \beta_i} = \prod_i p_i^{\min(\alpha_i, \beta_i)} \prod_i p_i^{\max(\alpha_i, \beta_i)}$

Exemple : $84 = 2^2 \times 3 \times 7$ et $70 = 2 \times 5 \times 7$

On vérifie que $84 \times 70 = 420 \times 14 = 5880$

2 Algorithmique

Problème

Etant donné un entier $n \geqslant 2$, déterminer une fonction (algorithmique) premier(n) telle que premier(n) retourne vrai si n est premier et faux sinon

Voici une première fonction

Algorithme 1 : Test de primalité

```
estPremier (n)
Données : un entier n > 2
Résultat : Vrai si n est premier faux sinon
1 début
2 |  pour chaque entier i tel que 2 ⩽ i ⩽ n − 1 faire
3 |  |  si i divise n alors
4 |  |  |  Retourner Faux
5 |  |  fin
6 |  fin
7 |  Retourner Vrai
8 fin
```

On mesure la *complexité* d'un algorithme en comptant le nombre d'instructions qui "prend le plus de temps " pour le processeur.

Une division prend plus de temps qu'une multiplication qui prend plus de temps qu'une addition.

Dans l'algorithme précédent on compte $n-1-2+1=n-2$ autrement dit à peu près n divisions on dit que l'algorithme a une complexité en $\mathrm{O}(n)$

En procédant ainsi on cherche à avoir des algorithmes de complexité la plus petite possible.

En tenant compte du lemme suivant donner une amélioration premier2(n) de la fonction précédente

Lemme 2 *Si $n \geqslant 2$ est composé alors il est divisible par un entier $a \leqslant \sqrt{n}$*

Preuve

Puisque n est composé il existe deux entiers $a,\ b$ différents de 1 et de n (a et b peuvent être confondus) tel que $n=ab$

L'un des deux a ou b est inférieur ou égal à $\sqrt{a}$ car sinon $a>\sqrt{n}$ et $b>\sqrt{n}$ font que $ab=n>n$ absurde

Algorithme 2 : Test de primalité

```
estPremier (n)
Données : un entier n > 2
Résultat : Vrai si n est premier faux sinon
1 début
2 |  pour chaque entier i tel que 2 ⩽ i ⩽ √n faire
3 |  |  si i divise n alors
4 |  |  |  Retourner Faux
5 |  |  fin
6 |  fin
7 |  Retourner Vrai
8 fin
```

En supposant que l'on puisse stocker en mémoire une certaine quantité de nombres premiers, voici une amélioration de premier2(n), où l'on ne divise n que par les nombres premiers $\leqslant \sqrt{n}$

Algorithme 3 : Test de primalité

```
estPremier (n)
Données : un entier n > 2
Résultat : Vrai si n est premier faux sinon
1 début
2 |  pour chaque premier i tel que 2 ⩽ i ⩽ √n faire
3 |  |  si i divise n alors
4 |  |  |  Retourner Faux
5 |  |  fin
6 |  fin
7 |  Retourner Vrai
8 fin
```

Cependant la quantité de nombres premiers que l'on peut stocker en mémoire est limitée (Voir exercice)

Voici un algorithme "ancien" pour engendrer les nombres premiers entre 2 et N où N est un entier "pas trop grand"

Crible d'Erathosthène

```
premier4(N)
   #On met dans une liste les nombres entiers de 2 à N
   liste    <- [2,....,N]
   premier_elt <- 2
   Tant qu'on n'a pas parcouru toute la liste
        Enlever de la liste tous les multiples de premier_elt
        premier_elt <- successeur(liste,premier_elt)
    retour liste
```

Exercice Appliquer premier4(50)

3 Test de primalité pour les "grands" entiers

Même problème que le 1 mais avec des "grands" entiers. Qu'est ce qu'un grand entier ? Une définition est un entier de plus de 100 chiffres

Théorème 5 (Petit théorème de Fermat) *Pour tout entier naturel a non multiple de tout nombre premier p on a $a^{p-1} \equiv 1\ [p]$*

Définition 3 (Nombre a-pseudo premier) *a un entier naturel supérieur ou égal à 2*

n est un nombre a-pseudo premier si $a^{n-1} \equiv 1\ [n]$ et n composé

Exemples :

1. 341 est un nombre 2-pseudo premier car $2^{340} \equiv 1[341]$ et $341 = 11 \times 31$
2. 121 est un nombre 3-pseudo premier car $3^{120} \equiv 1[121]$ et $121 = 11^2$
3. 15 est un nombre 4-pseudo premier car $4^{14} \equiv 1[15]$ et $15 = 3 \times 5$

Définition 4 (Nombres de Carmichaël (1912)) *Un nombre de Carmichaël est un nombre composé n tel que $a^{n-1} \equiv 1\ [n]$ pour tout a vérifiant :*
a premier avec n et $1 < a < n$

Exemple : Le plus petit nombre de Carmichaël est $561 = 3 \times 11 \times 17$

Théorème 6 ((Alford, Granville et Pomerance (1992))) *Il existe une infinité de nombres de Carmichaël*

Test probabiliste de primalité de Fermat
premierFermat(N)
choisir **au hasard** un nombre a entre 2 et n-1
si $a^{n-1} \equiv 1[n]$ retourner Vrai
Conclusion
On montre que lorsque N est grand plus de 100 chiffres le risque de se tromper est faible. Cependant Il existe des tests plus sûrs.

4 Densité des nombres premiers

On note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x
On admet que $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10^6) = 78\ 498$ et
$\pi(10^9) = 50\ 847\ 534$.

Gauss (1777-1855) conjectura que $\lim\limits_{x \to +\infty} \frac{\frac{\pi(x)}{x}}{\frac{1}{\ln(x)}} = 1$. Ce résultat ne fut démontré qu'un siècle plus tard en 1896 indépendamment par un mathématicien français Hadamard et un mathématicien belge De la Vallée Poussin. On regarde $\dfrac{\pi(x)}{x}$ comme **la densité de nombres premiers aux environs de** x