Les nombres premiers

Les nombres premiers sont aux entiers ce que les atomes sont aux molécules. Cependant contrairement au monde des molécules , les nombres premiers sont en quantité infinie !

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, ...

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 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 est il divisible par p_i ?.....

D'après le lemme 1, ...

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 n = 2, car 2 est premier

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

Si $n + 1$ est premier alors il n' y a rien à faire sinon il existe deux entiers q et p plus petits que n tel que $n + 1 = qp$, en appliquant l'hypothèse de récurrence sur q et p , $n + 1$ à son tour se décompose en produit de nombres premiers

Unicité

Par récurrence (forte) sur n

(Initialisation) Vrai pour n = 2

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

On sait que $n+1 = \prod_i p_i^{\alpha_i}$

pour pouvoir utiliser l'hypothèse de récurrence divisons $n+1$ par $p_0^{\alpha_0}$ (on a choisi un des nombres premiers dans la décomposition)

Par conséquent $n+1 = p_0^{\alpha_0} \times A$ et p_0 n'est pas dans la décomposition de A

Que peut-on dire de A ?

.....

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

Définition 2 *Deux entiers supérieurs ou égaux à 1 n et m, possèdent au moins un multiple commun leur produit nm*

Pourquoi peut on parler du plus petit commun multiple de n et m noté ppcm(m; n) ?

Théorème 3 $pgcd(\prod_{k=0}^{k=r} p_i^{\alpha_i} \ , \ \prod_{k=0}^{k=r} p_i^{\beta_i}) = \prod_{k=0}^{k=r} p_i^{\min(\alpha_i,\beta_i)}$

$ppcm(\prod_{k=0}^{k=r} p_i^{\alpha_i} \ , \ \prod_{k=0}^{k=r} p_i^{\beta_i}) = \prod_{k=0}^{k=r} p_i^{\max(\alpha_i,\beta_i)}$

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) = $2^2 \times 3 \times 5 \times 7 = 420$

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

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

2 Algorithmique

Problème 1

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

```
premier1(n)
```

```
pour i de 2 à n - 1
  si i divise n
     retourner vrai
retourner faux
```

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 .....

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 $\leqslant \sqrt{n}$

```
premier3(n)
  pour chaque premier p tel que p**2 <= n
    si p divise n
       retourner vrai
  retourner faux
```

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* $a^{p-1} \equiv 1\ [p]$

Preuve

On considère a tel que $\text{pgcd}(a, p) = 1$ Pourquoi ?

On considère la suite finie des multiples de a de a jusqu'à $(p-1)a$, c'est à dire :

$$a,\ 2a,\ 3a, ...,\ (p-1)a$$

Deux termes quelconque de cette suite finie ne peuvent pas être congrus modulo p car :

Si $ka \equiv k'a\ [p]$ alors $k \equiv k'\ [p]$ et finalement $k' = k$ (Le justifier)

Maintenant multiplions tous les termes de cette suite finie entre eux on obtient d'une part .....

et d'autre part en raisonnant modulo p .....

Pourquoi peut on éliminer $(p-1)!$ de part et d'autre du signe $\equiv$ et arriver à $a^{p-1} \equiv 1\ [p]$?

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.