**RECHERCHES SUR LES NOMBRES PREMIERS**

**Introduction**

* une notion de base en arithmétique
* un défi mathématique
* nombreuses applications (cryptologie, transmission de l’information)

**Objectif :**

* *étude d’une méthode personnelle pour obtenir théoriquement tous les nombres premiers, effectuant uniquement des opérations simples, et qui pourrait continuer indéfiniment*
* 257 885 161-1 (janvier 2013 ; + de 17 millions de chiffres)

**Plan :**

* **Définition et notations**

1. **Présentation de la méthode**
2. **Propriétés**
3. **Commentaires**

* **Conclusion**
* **Définition et notations**

On se place dans .

* *un nombre est dit premier*

*ssi ses seuls diviseurs dans sont 1 et lui-même.*

* Pi : le i-ième nombre premier (p1=2, p2=3, p3=5, p4=7,...)
* Pn#=

(7#=210, 11#=2310…)

1. **Présentation de la méthode**

-méthode par étape.

A l’étape i : Li = {p1, p2,…, pi}

Ti : le tableau obtenu initialement à l’étape i

Ti’ celui obtenu après modification de Ti.

**Initialisation**

* ***Etape 3 : c’est l’étape qui permet de comprendre le principe***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 7 | 11 | 13 | 17 | 19 | 23 | 29 |
| +5# | 31 | 37 | 41 | 43 | 47 | 49 | 53 | 59 |
| +5# | 61 | 67 | 71 | 73 | 77 | 79 | 83 | 89 |
| +5# | 91 | 97 | 101 | 103 | 107 | 109 | 113 | 119 |
| +5# | 121 | 127 | 131 | 133 | 137 | 139 | 143 | 149 |
| +5# | 151 | 157 | 161 | 163 | 167 | 169 | 173 | 179 |
| +5# | 181 | 187 | 191 | 193 | 197 | 199 | 203 | 209 |
| +5# | 211 | 217 | 221 | 223 | 227 | 229 | 233 | 239 |
| +5# | 241 | 247 | 251 | 253 | 257 | 259 | 263 | 269 |
| +5# | 271 | 277 | 281 | 283 | 287 | 289 | 293 | 299 |
| +5# | 301 | 307 | 311 | 313 | 317 | 319 | 323 | 329 |
| +5# | 331 | 337 | 341 | 343 | 347 | 349 | 353 | 359 |
| +5# | 361 | 367 | 371 | 373 | 377 | 379 | 383 | 389 |
| +5# | 391 | 397 | 401 | … |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

En passant d’une étape à l’autre, on enlève en fait à chaque fois une infinité de nombres que l’on aurait retrouvés si on n’utilisait que le crible d’Eratosthène.

**D’où est venue l’idée ?**

Nombres premiers primorielles :

5 ; 29 ; 2309 ; 30029

et 7 ; 31 ; 211 ; 2311 ; 223092671 ; 200 560 490 131

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 421 | 431 | 433 | 437 | 439 |  | 499 | 503 | 509 | 517 | 521 | 523 |
| 7#+a | 211 | 221 | 223 | 227 | 229 |  | 289 | 293 | 299 | 307 | 311 | 313 |
| **a** | **1** | **11** | **13** | **17** | **19** | **…** | **79** | **83** | **89** | **97** | **101** | **103** |
| 7#-a | 209 | 199 | 197 | 193 | 191 |  | 131 | 127 | 121 | 113 | 109 | 107 |

D’où l’idée que les nombres premiers pourraient peut-être se trouver à partir de tableaux…

1. **Propriétés**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 7 | 11 | 13 | 17 | 19 | 23 | 29 |
| +5# | 31 | 37 | 41 | 43 | 47 | 49 | 53 | 59 |
| +5# | 61 | 67 | 71 | 73 | 77 | 79 | 83 | 89 |
| +5# | 91 | 97 | 101 | 103 | 107 | 109 | 113 | 119 |
| +5# | 121 | 127 | 131 | 133 | 137 | 139 | 143 | 149 |
| +5# | 151 | 157 | 161 | 163 | 167 | 169 | 173 | 179 |
| +5# | 181 | 187 | 191 | 193 | 197 | 199 | 203 | 209 |

 : le nombre de colonnes.

Cela revient à compter les multiples de 7 que l’on va enlever.

* **Au plus un par colonne** (raisonnement par l’absurde : si on suppose qu’il y en a 2 : 7k et 7k’, il existe i de 1 à 6 tel que 7k=7k’+30i, ce qui est absurde car 7 ne divise pas 30i)
* **Au moins le nombre de colonnes** (7 × les éléments de la première ligne)
* **On en déduit :**

|  |  |
| --- | --- |
|  | Eléments de |
| + pn# |  |
| … |  |
| + pn# |  |

* lignes

Ainsi : .

Or

Donc :

Ce qui est vrai pour tout n.

Comme , on obtient le résultat.

1. **Commentaires**

**Etude de la répartition : comparaison avec le théorème des nombres premiers**

|  |  |  |  |
| --- | --- | --- | --- |
| Etape i | Pi+1# | x/log(x) | #Ti’ |
| 1 | 6 | 7 | 2 |
| 2 | 30 | 20 | 8 |
| 3 | 210 | 90 | 48 |
| 4 | 2 310 | 686 | 480 |
| 5 | 30 030 | 6 706 | 5 760 |
| 6 | 510 510 | 89 437 | **92 160** |
| 7 | 9 699 690 | 1 388 296 | 1 658 880 |
| 8 | 223 092 870 | 26 722 555 | 36 495 360 |
| 9 | 6 469 693 230 | 659 440 417 | 802 897 920 |

-même puissance de 10

**Apport de la programmation de l’algorithme sur Caml**

On a réussi actuellement à aller jusqu’à **l’étape 6.**

510 481 = p42 332 (en moins d’une seconde)

-**problème de stockage des nombres** (à l’étape 10, on comptera déjà un tableau avec 1 milliards d’éléments !)

92 160 - 42 332 = 49 828 nombres n’étaient pas premiers dans notre tableau. C’est plus de la moitié !

Avant d’enlever les multiples de pn+1, on ne peut affirmer à 100% qu’un nombre est premier que si celui-ci est inférieur à pn+12.

**Remarque sur les nombres premiers jumeaux**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 7 | **11** | **13** | **17** | **19** | 23 | **29** |
| +5# | **31** | 37 | **41** | **43** | 47 | 49 | 53 | **59** |
| +5# | **61** | 67 | **71** | **73** | 77 | 79 | 83 | 89 |
| +5# | 91 | 97 | **101** | **103** | **107** | **109** | 113 | 119 |
| +5# | 121 | 127 | 131 | 133 | **137** | **139** | 143 | **149** |
| +5# | **151** | 157 | 161 | 163 | 167 | 169 | 173 | **179** |
| +5# | **181** | 187 | **191** | **193** | **197** | **199** | 203 | 209 |

-très favorable à la conjecture : « il y a une infinité de nombres premiers jumeaux »

-il suffirait de montrer qu’il y a au moins un couple de nombres premiers jumeaux par tableau. Mais :

- 29 et 31 ; 209 et 211…bref : est dans Tn

- pas de régularité sur la position des nombres en vert

-> on ne peut pas conclure…

**Conclusion**

|  |  |
| --- | --- |
| Inconvénients | Avantages |
| * Problème de stockage * Complexité primorielle * On ne peut pas aller loin… | * Tous les nombres premiers sont obtenus * Que des opérations simples * Contrairement au crible d’Eratosthène, il n’y a pas de limite fixée : l’algorithme pourrait théoriquement tourner indéfiniment * Autre approche des nombres premiers. Cela permet de discuter sur la répartition et sur des conjectures actuelles… |

**ANNEXE**

* ***Etape 0 :***

.

|  |  |
| --- | --- |
|  | 1 |
| +1 | 2 |

* ***Etape 1 :***

.

|  |  |
| --- | --- |
|  | 1 |
| +2# | 3 |
| +2# | 5 |

Remarque sur 1 : par convention, on a décidé que 1 n’était pas premier. On voit bien effectivement avec le tableau que 1 occupe une place à part : lui, on ne l’enlève jamais (alors que tous les nombres premiers vont dans Ln). De plus, c’est à partir de lui que tout se construit (cf T0).

* ***Etape 2 :***

.

|  |  |  |
| --- | --- | --- |
|  | 1 | 5 |
| +3# | 7 | 11 |
| +3# | 13 | 17 |
| +3# | 19 | 23 |
| +3# | 25 | 29 |

Remarque : j’ai eu du mal à exprimer une cohérence dans les premières étapes car je voulais absolument que la méthode puisse s’appliquer en ne partant que de 1. Bien sûr la méthode pourrait se faire en initialisant à l’étape 3, celle qui permet de comprendre le principe, celle où l’on voit ce vraiment ce que l’on fait.

A voir éventuellement :

* Probabilité qu’un nombre soit premier -> cf Euclide et Polya
* Répartition des nombres premiers : construction d’Euclide ; théorème de Dirichlet (an+b)
* Test de Miller-Rabin ; méthode AKS ; crible d’Atkin…