ULCO **2018 - 2019**
L1 Mathématiques et Informatique **Calcul Formel**

TP 5 – Nombres premiers : crible d'Erathostène et répartition

Rappelons qu'un entier est dit premier s'il admet exactement deux diviseurs, c'est à dire si ses seuls diviseurs sont 1 et lui-même. L'ensemble des nombres premiers commence par 2,3,5,7,11,13,17,etc
Nous n'utiliserons pas dans un premier temps les commandes de `Maxima` qui est bien sûr capable de vous donner le milième nombre premier ou de tester si un nombre entier est un nombre premier. Même si vous les connaissez, ne les utilisez pas dans l'élaboration du crible d'Erathostène, cela n'aurait aucun sens.

Les premières questions qui viennent naturellement à l'esprit relativement aux nombres premiers sont :

1. comment trouver efficacement les nombres premiers?
2. Existe-t-il une infinité de nombres premiers?
3. S'il en existe une infinité, en existe-il beaucoup? Peut-on prévoir dans quelle proportion vont-ils apparaître?

Nous allons commencer à donner des réponses à ces trois questions dans cette séance. Commençons par la première.

1 Le crible d'Erathostène

Le crible d'Erathostène dans sa "version papier", consiste à suivre les démarches suivantes :

1. Choisir un entier M.
2. Placer tous les entiers de 1 à M dans un tableau T et ceci sur votre feuille de papier. On considère que 1 n'est pas premier, barrez-le.
3. Pour chaque entier k entre 2 et $\sqrt{M}$, on regarde si k est encore présent dans le tableau T. Si c'est le cas, alors k est un nombre premier et on barre tous ses multiples $k \cdot u$ avec u entre 2 et M/k.
4. A la fin de cette double boucle, le tableau T contient exactement les nombres premiers entre 2 et M.

Essayer sur une feuille avec un entier M raisonnable, disons $M = 50$. Constater qu'il ne reste sur votre feuille à la fin du crible que des nombres premiers. Comprendre les bornes et $\sqrt{M}$ et M/k des étapes 2 et 3. Si vous ne savez pas les retrouver, vous n'avez pas compris le crible.

Dans son implémentation avec `Maxima`, nous choisissons ici de considérer une liste `T` qui ne contient au départ que des 1. Si l'on veut déterminer tous les premiers jusque $M = 100$, on commencera donc par :

```
(%i1) M:100;
      T:makelist(1,k,1,M)$
      T[1]:0;
```

On a déjà indiqué ci-dessus que 1 n'est pas premier.

Barrer un entier i du tableau sera effectué dans votre programme en affectant 0 à la i-me place de la liste `T`. Par exemple, pour barrer 6, c'est à dire 2 fois 3, il vous faudra affecter dans votre programme `T[2*3]:0`.

1. Programmer le crible d'Erathostène à l'aide d'une double boucle. A la fin de cette première phase, vous disposerez de la liste `T` telle que pour tout i, `T[i]` égal à 1 est équivalent au fait que i est un nombre premier. Vérifier que votre programme fonctionne!

2. Créer avec `Maxima` une liste vide nommée `prem`. Puis, à l'aide d'une boucle, y ajouter itérativement les nombres premiers (quand T[i] vaut 1, l'entier i est premier et on l'ajoute à la liste prem avec la commande `endcons`). Vérifier que pour $M = 100$, vous obtenez la liste :

$$[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97]$$

3. Il est maintenant très facile de compter combien il y a de nombres premiers jusque un entier donné n : il suffit d'ajouter toutes les valeurs $T[1], T[2], \ldots$, jusque $T[n]$. Par exemple, il y a quatre nombres premiers jusque $n = 10$ car

$$T[1] + T[2] + \cdots + T[10] = 0 + 1 + 1 + 0 + 1 + 0 + 1 + 0 + 0 + 0 = 4.$$

   Créer un tableau appelé Pi par la commande `Pi:makelist(1,n,1,M)` (surtout ne mettez pas de % avant le nom `Pi`, il s'agit juste du nom Pi qui n'a pas grand chose à voir ici avec π). Puis, à l'aide d'une boucle, calculez tous les entiers `Pi[n]` donnant le nombre de nombres premiers jusque n. Après votre boucle, vérifier que `P[10]` vaut 4, `P[100]` vaut 25 car il y a 25 nombres premiers inférieurs ou égaux à 100.

4. On veut représenter par un graphique les quantités de nombres premiers jusqu'aux entiers n ceci pour $n = 1, \ldots, M$. Créer la liste `pts` des points de coordonnées `[n,Pi[n]]` pour $n = 1, \ldots, M$. Puis, tracer un graphique réprésentant ces points.

5. Hadamard et La Vallée Poussin ont démontré en 1896, et ceci indépendamment l'un de l'autre, un des résultats les plus célébres de la théorie des nombres : le théorème de répartition des nombres premiers.

   Dans ce théorème, la fonction $\Pi : \mathbb{R} \to \mathbb{N}$ compte le nombre de nombres premiers inférieurs ou égaux à x. Elle coïncide sur les entiers avec les valeurs de notre liste `Pi` définie en 3. Par exemple, $\Pi(10) = 4$, $\Pi(100) = 25$, $\Pi(1000) = 168$.

   Théorème 1. Le nombre $\Pi(x)$ de nombres premiers inférieurs ou égaux à x est équivalent, lorsque le réel x tend vers $+\infty$, au quotient de x par son logarithme népérien :

$$\Pi(x) \sim \frac{x}{\ln(x)}$$

   ce qui signifie que

$$\lim_{x \to +\infty} \frac{\Pi(x)}{\frac{x}{\ln(x)}} = 1$$

   Reprendre par un Copier/Coller les commandes du graphique obtenu en question 4. Ajouter à ce graphique le graphe de la fonction $x \to x/\ln(x)$. Vous serez peut-être un peu déçus par le graphe obtenu car notre intuition des fonctions équivalentes ne correspond pas à ce qu'elles sont parfois. Deux fonctions f et g peuvent être équivalentes, c'est à dire vérifier $\lim f(x)/g(x) = 1$ mais aussi vérifier $\lim_{x\to\infty} f(x) - g(x) = \infty$.

2 La preuve d'Euclide de l'infinitude des premiers

La question de savoir s'il existe une infinité de nombre premiers est une des premières qui a du vous venir à l'esprit en commençant à manipuler ces entiers si particuliers. Euclide (-300 avant J.C.) démontre qu'il en existe effectivement une infinité.
Notons que l'infinitude des premiers est équivalente au fait que la limite de $\Pi(x)$ vaut $+\infty$ quand x tend vers l'infini. Or, le théorème de répartition des nombres premiers donne l'implication

$$\Pi(x) \sim \frac{x}{\ln(x)} \implies \lim_{x\to\infty} \Pi(x) = +\infty \text{ car } \lim_{x\to\infty} \frac{x}{\ln(x)} = +\infty$$

Nous venons ci-dessus d'utiliser un rouleau compresseur pour écraser une noix... Essayons plutôt de comprendre l'argument d'Euclide. Le procédé est très simple et très astucieux:
Soit $n > 1$ un entier et notons $p_1, p_2, \ldots, p_n$, les n premiers nombres premiers consécutifs. Considérons l'entier

$$X = p_1 p_2 \cdots p_n + 1$$

• Si X est premier, nous avons trouvé un nombre premier plus grand que p_n.
• Si X n'est pas premier, il peut être factorisé en écrivant $X = v \cdot q$ avec q un nombre premier strictement entre 1 et X. Montrons que q est strictement plus grand que p_n : Par l'absurde, si ce n'est pas le cas alors q est un nombre premier inférieur ou égal à p_n et et il est donc un des nombres premiers p_l avec $1 \leq l \leq n$. Il vient alors

$$X = vq = vp_l = p_1 p_2 \cdots p_l \cdots p_n + 1$$

Ce qui implique

$$p_l(v - p_1 p_2 \cdots p_{l-1} p_{l+1} \cdots p_n) = 1$$

Or, si un produit d'entier est égal à 1 alors les deux entiers sont égaux à ± 1. Ce n'est pas possible car p_l est un nombre premier. Nous venons de montrer que notre hypothèse est fausse : q est stritement plus grand que p_n.
Faisons le point : si vous prenez les n premiers nombres premiers et que vous calculez X, vous trouverez automatiquement (par un des deux bullets précédents) un nombre premier plus grand que tous ceux que vous aurez considérés : il ne peut exister un nombre fini de nombres premiers. Ce qui termine la preuve.

Prenons quelques exemples :
i : Existe-t-il un nombre premier plus grand que 2 et 3? On prend $X = 2 \cdot 3 + 1 = 7$. L'entier X est premier et est plus grand que 2 et 3.
ii : Existe-t-il un nombre premier plus grand que $2, 3, 5$ et 7? On prend $X = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$. L'entier X est premier et est plus grand que $2, 3, 5$ et 7.
iii : Continuons jusque 13, et on trouve cette fois-ci avec `Maxima` que X n'est pas premier mais qu'il admet pour facteurs 59 et 509 qui sont bien plus grands que $2, 3, 5, 7, 11, 13$.