TP4
Arithmétique

21 décembre 2017

Réalisé par RAHARIJAONA Dylan et KUCAM Delphine

Encadré par Jean-Paul Cardinal

1. Un nombre est-il premier ?

   (a) En cherchant sur Internet, on trouve que, dans les anciennes versions de Python, il suffit d'un slash/ pour obtenir le quotient d'une division euclidienne d'un entier par un autre mais pour les versions plus récente de Python, il faut dédoubler le slash. Ici, on peut se contenter d'un seul slash.
   Pour calculer le reste de la division euclidienne sur Python, on utilise l'opérateur infixé %. Cela permet de travailler sur les congruences.

   (b) <u>Définition</u> : Un nombre premier est un entier naturel qui admet exactement 2 diviseurs distincts entier et positifs (qui sont 1 et lui-même).

   (c) Nous cherchons à savoir quels sont les nombres premiers parmis ces nombre : 1001, 2017, 3001, 49999, 89999
   - Commençons par 1001 : en cherchant des diveurs de 1001, on trouve que 1001 = 3 x 143 ainsi 1001 n'est pas un nombre premier.
   - 2017, 3001, 49999 n'admettant pas de d'autres diviseurs entier et positifs que 1 et eux même, on peut conclure que ce sont bien des nombres premiers.
   - Quant à 89999, on trouve que 7 x 12857 = 89999 ainsi ce n'est pas un nombre premier

   (d) Nous devons écrire une fonction is-prime sur Python permettant de savoir si un nombre est premier ou non. Pour cela, nous avons d'abord raisonné par algorithme, c'est-à-dire :

   Entree :Un entier naturel n
   Sortie :true si n est premier, false sinon.
   Si n=0 ou n=1 Alors
   Retourner false
   Fin Si
   Si n=2 Alors
   Retourner true
   Fin Si
   p=2
   Tant Que $p \leq \sqrt{n}$ et p ne divise pas n Faire
   p=p+1
   Fin Tant Que
   Si p divise n Alors
   Retourner false
   Sinon
   Retourner true
   Fin Si

   Puis grâce à cet algorithme, nous nous sommes inspirés de ce modèle pour écrire la fonction is-prime sur Python.

(e) Nous cherchons à savoir si les 6 premiers nombres de Fermat sont premiers ou non. On a :
- $F_0 = 2^1 + 1 = 3$
- $F_1 = 2^2 + 1 = 5$
- $F_2 = 2^4 + 1 = 17$
- $F_3 = 2^8 + 1 = 257$
- $F_4 = 2^{16} + 1 = 65537$
- $F_5 = 2^{32} + 1 = 4294967297$

Nous savons que F_0, F_1, F_2, F_3 et F_4 sont premiers grâce à la fonction is-prime, pour F_5, on obtient "false", en effet 4294967297 n'est pas premier.

2. Crible d'Eratosthène, distribution des nombres premiers

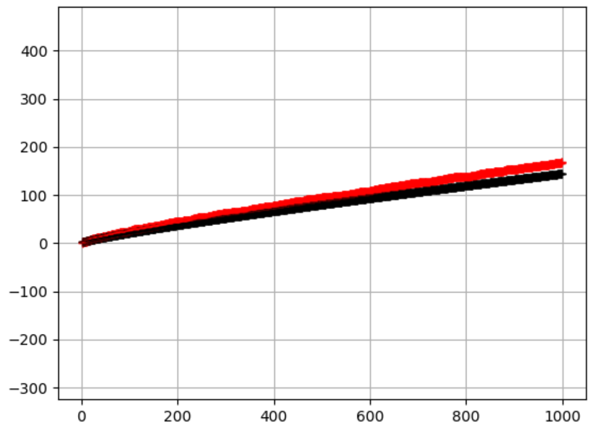
(a) Nous avons fait une petite recherche sur le crible d'Eratosthène afin d'en savoir plus à ce sujet. Pour calculer la liste de tous les nombres premiers inférieurs à 200, il suffit de :
1. écrire tous les entiers de 2 à 200
2. enlever les multiples de 2 sauf 2
3. récupérer le plus petit nombre non barré et barrer ses multiples
4. on s'arrête dès qu'on a atteint la racine carré de 200
Nous l'avons fait sur papier et nous vous l'avons rendu en main propre.

(b) Pour cette question nous devons créer une fonction *primes* qui prend en argument un entier n et qui renvoie la liste de tous les premiers inférieurs à n. Au début, on a créer une boucle for et malheuresement il y avait un problème de taille que nous n'avons pas réussi à résoudre. Ducoup, nous avons demander de l'aide au professeur qui nous a débloqué.

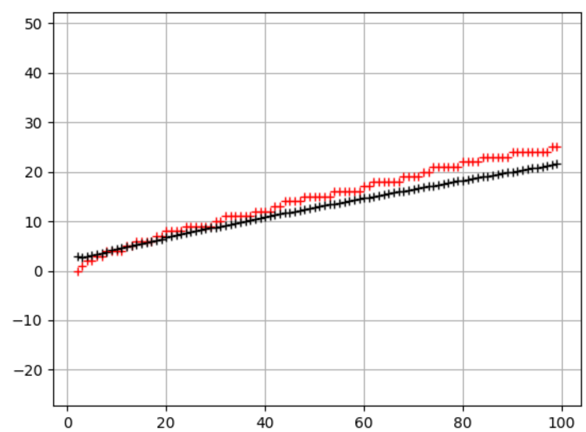
(c) Nous avons calculé la liste de tous les premiers inférieurs à 1000 à l'aide de la fonction *primes* (créer précédemment). Voici ce que l'on obtient :

```
tableau des premiers inferieurs a 1000
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  101  103  107  109  113
127  131  137  139  149  151  157  163  167  173
179  181  191  193  197  199  211  223  227  229
233  239  241  251  257  263  269  271  277  281
283  293  307  311  313  317  331  337  347  349
353  359  367  373  379  383  389  397  401  409
419  421  431  433  439  443  449  457  461  463
467  479  487  491  499  503  509  521  523  541
547  557  563  569  571  577  587  593  599  601
607  613  617  619  631  641  643  647  653  659
661  673  677  683  691  701  709  719  727  733
739  743  751  757  761  769  773  787  797  809
811  821  823  827  829  839  853  857  859  863
877  881  883  887  907  911  919  929  937  941
947  953  967  971  977  983  991  997
```

(d) Ceci est le graphique représentant $\pi(n)$ (en rouge) et $\dfrac{n}{\log n}$ en fonction de n (en noir) pour n allant de 2 à 1000.



Voici ce que l'on obtient plus précisément (pour n allant de 2 à 100).



n	pi(n)	n/log n
10	4	4.34294481903
100	25	21.7147240952
1000	168	144.764827301
10000	1229	1085.73620476
100000	9592	8685.88963807
1000000	78498	72382.4136505

(e)

3. Factorisation d'un entier en premiers

   (a) Théorème fondamental de l'arithmétique : tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

   (b) Voici la décomposition de 924 en produits de facteurs premiers : 924 = 2*462 = 2*2*231 = 2*2*3*77= 2*2*3*7*11.

4. pgcd de deux entiers, identité de Bézout, algorithme d'Euclide

   (a) Le plus grand commun diviseur ou PGCD de deux nombres entiers non nuls est le plus grand entier qui les divise simultanément.

   (b) On veut trouver le pgcd de 4864 et 3458 en décomposant en facteurs premiers, on obtient :

   4864 = 2 x 2 x 2 x 2 x 2 x 2 x 2 x 2 x 19
   3458 = 2 x 7 x 13 x 19

   Ainsi le pgcd de 4864 et 3458 est 2x19 soit 38.

   (c) L'identité de Bézout est un résultat d'arithmétique élémentaire, qui prouve l'existence de solutions à l'équation diophantienne linéaire :

   ax + by = pgcd(a, b)

   d'inconnues x et y entiers relatifs, où a et b sont des coefficients entiers relatifs et où pgcd(a, b) est le plus grand commun diviseur de a et b.

(d) Nous cherchons x et y :

$$
\begin{aligned}
4864 &= 1 \text{ x } 3458 + 1406 \\
3458 &= 2 \text{ x } 1406 + 646 \\
1406 &= 2 \text{ x } 646 + 114 \\
646 &= 5 \text{ x } 114 + 76 \\
114 &= 1 \text{ x } 76 + 38 \\
76 &= 2 \text{ x } 38 + 0
\end{aligned}
$$

$$
\begin{aligned}
&114 - 1 \text{ x } 76 = 38 \\
&114 - 1(646 - 5 \text{ x } 114) = 38 \\
&-1 \text{ x } 646 + 6 \text{ x } 114 = 38 \\
&-1 \text{ x } 646 + 6(1406 - 2 \text{ x } 646) = 38 \\
&-13 \text{ x } 646 + 6 \text{ x } 1406 = 38 \\
&6 \text{ x } 1406 - 13(3458 - 2 \text{ x } 1406) = 38 \\
&-13 \text{ x } 3458 + 32(4864 - 3458) = 38 \\
&32 \text{ x } 4864 - 45 \text{ x } 3458 = 38
\end{aligned}
$$

A l'aide de l'algorithme de Bézout, on trouve x = 32, y = -45 et d = 38

5. Pour cette question, j'ai travaillé avec Aboubakr jusque la question f et nous avons décidé de s'arrêter là pour commencer nos projet.