ÉNS de Lyon — Option C
2018-2019 — Agrégation

TP2 : tests de primalité

Exercice 1 — **1.** Écrire un programme prenant en entrée deux entiers a et n et qui teste si a est un témoin de Miller pour n.

2. Programmer un test prenant en entrée deux entiers n et k, qui teste k nombres « aléatoires » entre 2 et $n-1$ et qui renvoie « composé » si l'un de ces nombres est un témoin de Miller et « probablement premier » sinon.

3. Programmer le test de primalité de Lucas-Lehmer pour les nombres de Mersenne.

4. Comparer les vitesses d'exécution de ces deux tests en utilisant « a%n » et « IntegerModRing(n)(a) ».

5. Comparer les vitesses de ces tests avec le test « is_prime » et « is_pseudoprime ».

Exercice 2 —Nombres de Carmichael

1. Écrire un programme prenant en entrée un entier n et déterminant si n est un nombre de Carmichael (en utilisant is_prime), en utilisant le critère de Korselt (n est de Carmichael si et seulement si n n'est pas premier, n est sans facteurs multiples et pour tout diviseur premier p de n, $p-1$ divise $n-1$).

2. Écrire un programme probabiliste prenant en entrée deux entiers n et k et déterminant si n est probablement un nombre de Carmichael ou s'il ne l'est pas, en vérifiant s'il existe des témoins de Fermat, et en utilisant le fait que si n n'est pas un nombre de Carmichael, au moins la moitié des $a \in [\![1, n-1]\!]$ sont des témoins de Fermat.

3. Donner la liste des nombres de Carmichael inférieurs à 10^6.

4. Pour $n \in \mathbb{N}_{\geq 2}$, on note $C(n)$ le nombre de nombre de Carmichael inférieurs à $100n$ et $\pi(n)$ le nombre de nombre premiers inférieurs à $100n$.

Sur un même graphe, tracer le graphe de C en bleu et le graphe de π en rouge.

Tracer le graphe de $\frac{\pi(n)}{C(n)+\pi(n)}$.

Exercice 3 — **1.** Écrire un programme prenant en entrée un entier n et donnant le plus petit nombre premier plus grand que n. Comparer avec les fonctions « next_prime » et « next_probable_prime ».