Tests de primalité

Exercice 1 *Tests de Fermat et Miller–Rabin*

1. Écrire une procédure `test_prim_fermat(n)` implémentant le test de primalité de Fermat pour un entier impair n. Comparer avec `is_prime`, notamment pour l'entier $n = 561$.
2. Écrire une procédure `test_prim_mira(n)` implémentant le test de primalité de Miller–Rabin pour un entier impair n (on pourra utiliser la commande `L.index(a)` renvoyant la première occurence de l'élément a dans la liste L). Tester cette procédure pour $n = 561$ et $m = 9\,746\,347\,772\,161$. Comparer avec la réponse du test de Fermat pour m.
3. Écrire un raffinement `test_prim_mira2(n,k)` de la procédure précédente prenant en entrée un entier impair $n \geqslant 1$ et un entier $k \geqslant 1$ et détectant correctement la primalité de n, ou sa non primalité, ou bien produisant un diviseur non trivial de n, avec probabilité d'erreur inférieure à $1/2^k$.
4. Comparer les vitesses d'exécution de `test_prim_mira2` et `is_prime` pour de « grands » entiers impairs n. On utilisera la fonction `time` de `Sage` ; à titre d'essai et de comparaison avec le coût d'un test de primalité, on pourra faire exécuter

```
time factor(next_prime(2^90)*next_prime(2^92))
```

Exercice 2 *Test de Solovay–Strassen*

1. Écrire une procédure `test_prim_sostra(n)` implémentant le test de primalité de Solovay–Strassen pour un entier impair n. On utilisera la fonction `kronecker` de `Sage` permettant le calcul des symboles de Jacobi.
2. Écrire une procédure `symbole_de_jacobi(a,b)` implémentant le calcul récursif du symbole de Jacobi $\left(\frac{a}{b}\right)$, pour des entiers impairs $a \geqslant 1$ et $b \geqslant 1$.
3. Incorporer la procédure `symbole_de_jacobi` dans la procédure `test_prim_sostra` pour éviter le recours à la fonction `kronecker` de `Sage`.

Exercice 3 *Nombres de Carmichael*

1. Montrer que tout nombre de Carmichael $n \geqslant 3$ a la propritété suivante : pour tout diviseur premier p de n, on a $(p-1) \mid (n-1)$ (on pourra fixer un générateur de $\mathbf{F}_p^\times$ et appliquer le théorème des restes chinois).
2. Montrer que n est un nombre de Carmichael si et seulement si n est un entier sans facteur carré non premier et vérifiant la propriété de la question 1. En déduire un test `test_car(n)` (utilisant par exemple la fonction `factor` accompagnée de la commande `list`) permettant de déterminer si n est un nombre de Carmichael ou non. Tester cette procédure pour les entiers : 663, 867, 935, 1105, 1547, 1729, 2077, 2465, 2647, 2821, 172081.
3. Montrer qu'un nombre de Carmichael est toujours impair et admet au moins trois facteurs premiers.

4. Soient $p_1 = 6m + 1$, $p_2 = 12m + 1$ et $p_3 = 18m + 1$ trois entiers dont on suppose qu'ils sont premiers pour une certaine valeur de m. Montrer que pour cette valeur de m l'entier $p_1p_2p_3$ est un nombre de Carmichael.
5. En utilisant un test de primalité (extrait de l'exercice 1 par exemple, ou bien en ayant recours à `is_prime`), déterminer les 5 plus petits nombres de Carmichael de la forme donnée à la question précédente.

Exercice 4 *Primalité des nombres de Mersenne*

Soit p un nombre premier. Le p-ième nombre de Mersenne est l'entier $M_p = 2^p - 1$.

1. Déterminer un nombre de Mersenne premier et un nombre de Mersenne composé (on notera par ailleurs que si n est composé alors $2^n - 1$ l'est aussi).
2. On appelle suite de Lucas–Lehmer la suite d'entiers $(s_n)_{n\geqslant 0}$ définie par

$$s_0 = 4\,, \qquad s_{i+1} = s_i^2 - 2\,,\ i \geqslant 0\,.$$

   En admettant la propriété suivante : M_p est premier si et seulement si $s_{p-2} \equiv 0(\bmod M_p)$, implanter un test `prem_mers(p)` prenant en entrée un nombre premier p (ou en supposant simplement p entier et en testant au préalable sa primalité via un des tests étudiés dans cette feuille) et testant la primalité de M_p.
3. Dans cette question et la suivante on souhaite démontrer le critère de primalité de la question précédente. Commencer par vérifier que pour tout i, on a $s_i = \omega^{2^i} + \overline{\omega}^{2^i}$ où $\omega = 2 + \sqrt{3}$ et $\overline{\omega} = 2 - \sqrt{3}$. Supposons maintenant $s_{p-2} \equiv 0(\bmod M_p)$.
   (a) Montrer qu'il existe un entier k tel que $\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1$. Par l'absurde, on suppose désormais M_p composé. Notons q le plus petit facteur premier de M_p.
   (b) On a un morphisme d'anneaux $\varphi : \mathbf{Z}[\sqrt{3}] \to \mathbf{F}_q[t]/(t^2 - 3)$. Montrer que $\varphi(\omega)$ est d'ordre 2^p dans le groupe des inversibles de $\mathbf{F}_q[t]/(t^2 - 3)$.
   (c) Déduire une contradiction.
4. Réciproquement supposons M_p premier. On admet par ailleurs que 3 est un non-carré modulo M_p.
   (a) Montrer que 2 est un carré modulo M_p.
   (b) Notons $\sigma = 2\sqrt{3}$ dans le corps $\mathbf{F}_{M_p}(\sqrt{3})$. Montrer que $(6 + \sigma)^{M_p} = 6 - \sigma$.
   (c) Notons $\omega = (6 + \sigma)^2/24$. Montrer que $\omega^{\frac{M_p+1}{2}} = -1$.
   (d) Conclure que $s_{p-2} \equiv 0\,(\bmod M_p)$ en multipliant cette dernière inégalité par $\overline{\omega}^{\frac{M_p+1}{4}}$ où $\overline{\omega}$ désigne l'inverse de ω.