Autour de la primalité

Test de primalité de Lucas-Lehmer pour les nombres de Mersenne

0. Soient a et n deux entiers strictement plus grands que 1. Donner une condition nécessaire sur a et n pour que $a^n - 1$ soit premier. Cette condition est-elle suffisante ? On pourra expérimenter avec Sagemath.

Un *nombre de Mersenne* est un entier de la forme $m = 2^p - 1$, où p est un nombre premier. On s'intéresse surtout aux nombres de Mersenne qui sont eux-même premiers.

1. Expliquer pourquoi l'arithmétique modulo $2^p - 1$ est particulièrement rapide.
2. Soit $m = 2^p - 1$ un nombre de Mersenne premier. Démontrer que $n = 2^{p-1}m$ est un nombre parfait, c'est-à-dire qu'il est égal à la somme de ses diviseurs stricts :

$$n = \sum_{\substack{d|n \\ 1 \leq d < n}} d$$

(On sait montrer depuis Euler que tous les nombres parfaits pairs sont de cette forme. Par ailleurs, on ignore encore s'il existe des nombres parfaits impairs.)

On dispose d'un critère très efficace pour déterminer si un nombre de Mersenne est premier [1] :

Théorème (Lucas–Lehmer)**.** *Soit p un nombre premier. On considère la suite $(s_k)_{k\in\mathbb{N}}$ définie par :*

$$\begin{cases} s_0 = 4 \\ \forall k \in \mathbb{N},\ s_{k+1} = s_k^2 - 2 \end{cases}$$

Alors le nombre de Mersenne $m = 2^p - 1$ est premier si et seulement si $s_{p-2} = 0 \bmod m$.

3. Écrire un programme qui utilise le théorème précédent pour déterminer si un nombre de Mersenne est premier. Quelle est la complexité de ce test ?
   Utiliser ce programme pour trouver tous les nombres de Mersenne premiers de moins de 1000 bits.
4. Montrer que $s_k = (2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k}$ pour tout $k \in \mathbb{N}$.

On considère dans la suite les éléments $\omega = 2 + X$ et $\bar{\omega} = 2 - X$ de $\mathbb{Z}[X]$.

5. Calculer $\omega\bar{\omega} \bmod X^2 - 3$. Montrer que $\omega^{2^k} + \bar{\omega}^{2^k} = s_k \bmod X^2 - 3$, pour tout $k \in \mathbb{N}$.
6. Preuve du théorème : condition suffisante.
   On suppose que $s_{p-2} = 0 \bmod m$ (avec $m = 2^p - 1$). On note q le plus petit facteur premier de m.
   (a) Montrer que $\omega^{2^{p-1}} = -1 \bmod (m, X^2 - 3)$
   (b) Montrer que (la classe de) ω est inversible dans le quotient $A = (\mathbb{Z}/q\mathbb{Z})[X]/(X^2 - 3)$, et donner son ordre multiplicatif.

1. Référence : P. Saux Picard, E. Rannou, Cours de calcul formel : Corps finis, systèmes polynomiaux, applications

(c) Montrer que $2^p \leq q^2 - 1$. En déduire que $m = q$, et donc que m est premier.

7. Preuve du théorème : condition nécessaire.
On suppose que $m = 2^p - 1$ est premier, avec $p > 2$. On admettra (loi de réciprocité quadratique) que si $n > 3$ est premier, alors 3 est un carré modulo n si et seulement si $n = 1$ ou 11 mod 12.
   (a) Déterminer la valeur de m modulo 3 puis modulo 4. En déduire que $3^{(m-1)/2} = -1 \bmod m$.
   (b) En calculant $(2^{(p+1)/2})^2 \bmod m$, montrer que 2 est un carré modulo m.
   En déduire la valeur de $2^{(m-1)/2} \bmod m$, puis de $6^{(m-1)/2} \bmod m$.
   (c) Démontrer que $(3 + X)^m = 3 - X \bmod (m, X^2 - 3)$.
   (d) En utilisant que $\omega = \frac{(3+X)^2}{6} \bmod X^2 - 3$, obtenir que $\omega^{(m+1)/2} = -1 \bmod (m, X^2 - 3)$.
   (e) Multiplier des deux côtés par $\bar{\omega}^{(m+1)/4}$ pour démontrer la relation :

$$\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = 0 \bmod (m, X^2 - 3).$$

   (f) Conclure.

Ordre et générateurs

8. Écrire une fonction qui prend en argument trois entiers (non nuls) a, k et n et teste si l'ordre de a dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal à k, en se servant de la factorisation de k. On renverra `False` si $a \wedge n \neq 1$.

9. Soit $n \geq 2$ un entier. Rappeler la condition pour que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ soit cyclique. Écrire un programme (probabiliste) qui, si cette condition est vérifiée, renvoie un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Pocklington

Un *certificat de primalité de Pocklington* pour un entier premier n est la donnée d'une liste de triplets (p_i, m_i, a_i) où les p_i sont des nombres premiers tels que le produit $p_1^{m_1} \dots p_s^{m_s}$ divise $n - 1$ et est plus grand que $\sqrt{n}$, et que pour tout $1 \leq i \leq s$,

$$a_i^{n-1} = 1 \bmod n \quad \text{et} \quad \operatorname{pgcd}(a_i^{(n-1)/p_i} - 1, n) = 1$$

10. Vérifier que les triplets $(2, 3, 7), (3, 3, 2), (5, 2, 2)$ certifient la primalité de 5 578 201.
11. Expliquer comment il est possible de se contenter d'une liste de couples (p_i, a_i).
12. Le triplet $(91, 1, 64)$ certifie-t-il la primalité de 4187 ? Quelle est la difficulté et comment peut-on y remédier ?
13. Trouver des exemples plausibles de faux certificats de Pocklington comme ci-dessus, qui tromperaient respectivement un vérificateur :
   — ne s'assurant pas de la primalité des p_i ;
   — ne s'assurant pas de la condition $\prod_i p_i^{m_i} > \sqrt{n}$;
   — ne s'assurant pas de la condition $p_i | n - 1$ (le calcul de $(n-1)/p$ renvoyant alors le quotient de la division euclidienne dans $\mathbb{Z}$).