TP2 - Loi de réciprocité quadratique et tests de primalité

09 octobre 2020

Les TPs comportent une partie à faire sur feuille (explicitement indiquée), ainsi qu'une partie implémentation.

L'objectif de ce TP est de manipuler la loi de réciprocité quadratique (et comprendre l'origine du nom) et de prendre connaissance de tests de primalité probabiliste.

> Sur `sage`, vous pouvez obtenir la documentation d'une fonction/méthode en ajoutant un '?' à la fin, ou en tapant `help(cmd)`, où `cmd` est la commande en question.
> N'oubliez pas d'abuser de l'autocompletion pour prendre connaissance des méthodes disponibles sur un objet donné.

Exercice 1 : Loi de réciprocité quadratique

La façon la plus intuitive de pensez pousse souvent à se demander, pour un nombre premier p fixé, quels entier q sont des résidus quadratique modulo p. Ici nous abordons le problème sous un angle différent : pour un entier $q > 2$ premier, quels sont les p tels que q est un résidu quadratique modulo p.

1. Soit $q \equiv 1 \bmod 4$, montrez que q est un résidu quadratique modulo $p \Leftrightarrow p \equiv r \bmod q$, où r est un résidu quadratique modulo q.
   Utilisez la loi de réciprocité quadratique.
2. Soit $q \equiv 3 \bmod 4$, montrez que q est un résidu quadratique modulo $p \Leftrightarrow p \equiv \pm b^2 \bmod 4q$, où b est un entier impair premier avec $q \neq p$.
   (a) Côté $\Leftarrow$: Si $p \equiv b^2 \bmod 4q$, montrez qu'on a $p \equiv 1 \bmod 4$ et $p \equiv b^2 \bmod q$. En déduire que q est un résidu quadratique modulo p. Raisonnez de manière similaire si $p \equiv -b^2 \bmod 4q$.
   (b) Côté $\Rightarrow$: Si q est un résidu quadratique modulo p, utilisez la loi de réciprocité pour déduire des informations sur les valeurs possibles de $\left(\frac{p}{q}\right)$ et observer $p \bmod 4$ et $p \bmod q$ pour obtenir le résultat souhaité.
3. En utilisant les résultats précédents et la loi de réciprocité quadratique, donnez la condition sur un nombre premier p pour que 7 soit un résidu quadratique modulo p.
   Observer les résidus quadratiques modulo 7 vous sera utile.

Exercice 2 : Calcul du symbole de Jacobi

L'algorithme suivant permet de calculer le symbole de Jacobi de deux entier a et b.

Algorithme 1 : JacobiSymbol(a, b)

1 $a \leftarrow a \bmod b$;
2 **while** $a \equiv 0 \bmod 2$ **do**
3 | Extraire le facteur 2 de a, et mettre à jour le résultat en conséquence;
4 **end**
5 **if** $a == 1$ **then**
6 | **return** 1;
7 **end**
8 **if** $pgcd(a, b) \neq 1$ **then**
9 | **return** 0;
10 **end**
11 $a, b \leftarrow swap(b, a)$ # Attention, le swap peut changer le signe du résultat;
12 goto 1;

1. À l'aide des propriétés du symbole de Jacobi, justifiez que la ligne 1 et 3 n'impacte pas le résultat.
2. Quelle(s) différence(s) notable(s) notez-vous entre entre le calcul du symbole de Jacobi et celui de Legendre ?
3. Implémentez l'algorithme précédent.

Exercice 3 : Test de composition de Solovay-Strassen

D'après le critère d'Euler, on sait que si n est un premier impair, alors pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$:

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$$

Si n n'est pas premier, un entier a qui vérifie l'égalité précédente est appelé un menteur d'Euler. Inversement, un entier a qui ne vérifie pas cette égalité est un témoin d'Euler et permet de conclure que n n'est pas premier. Le test de primalité de Solovay-Strassen consiste à tirer aléatoirement k éléments $a_i \in (\mathbb{Z}/n\mathbb{Z})^*$, et si l'égalité est vérifiée pour tout i, on en déduit que n est probablement premier. Sinon on conclut que n est composé. Pour des applications cryptographiques, $k = 50$ suffit.

1. Justifiez que le fait de trouver un témoin de composition permet de conclure que n n'est pas premier.
2. Montrez que pour un entier non premier n, les menteurs d'Euler représentent au plus la moitié de $(\mathbb{Z}/n\mathbb{Z})^*$. Notons
$$J_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n\}$$
Notre but est donc de montrer que $|J_n| \leq 0.5 \times |(\mathbb{Z}/n\mathbb{Z})^*|$.
   (a) Montrez que J_n est un groupe en vous servant des propriétés du symbole de Jacobi.
   (b) En raisonnant par contradiction, montrer que $J_n \neq (\mathbb{Z}/n\mathbb{Z})^*$.
      1. Considérez la factorisation de n en nombre premiers : $n = p_1^{k_1} \cdots p_t^{k_t}$. Notons $q = p_1^{k_1}$ et $m = n/q$. Soit g un générateur de $(\mathbb{Z}/q\mathbb{Z})^*$. Montrez qu'il existe $a \in (\mathbb{Z}/n\mathbb{Z})^*$ tel que $a \equiv g \bmod q$ et $a \equiv 1 \bmod m$.
      2. Considérez le cas où $k_1 = 1$. En calculant le symbole de Jacobi de a et n, déduire une contradiction.
      3. Considérez le cas où $k_1 \geq 2$. Montrez qu'un supposant $J_n = (\mathbb{Z}/n\mathbb{Z})^*$, on abouti à la conclusion que $p_1|n$ et $p_1|(n-1)$.
   (c) En déduire le résultat attendu.
3. Implémentez ce test.
4. Lancez votre test sur tous les entiers inférieurs à 1000, en vérifiant la véracité de votre résultat (avec la fonction `is_prime` par exemple). Que remarquez vous ?

Il existe une infinité de nombres appelés "nombres de Carmichael". Ces nombres sont de la forme n non premier tel que $a^{n-1} \equiv 1 \bmod n$ pour tout a premier avec n.
Il est évident que ces nombres passent le test de primalité de Fermat, malgré le fait qu'ils soient composés.

Exercice 4 : Test de Miller-Rabin

Une version plus évoluée de ce test permet de mettre au point un test de primalité probabiliste plus fiable.
Pour cela, il faut utilisé une variante du petit Théorème de Fermat que vous allez démontrer.

1. Soit p un nombre premier. Notons $p - 1 = 2^s q$ avec q impair. Montrez que, en vous servant du petit théorème de Fermat, que pour un entier $a < p$, premier avec p, nous avons deux possibilités :

   (i) $a^d \equiv 1 \bmod p$

   (ii) $\exists r \in [0, s-1]$ tel que $a^{2^r q} \equiv -1 \bmod p$

   Un entier qui ne satisfait aucune de ces deux propositions est composite. Le test de Miller-Rabin consiste à répéter ce test avec différentes valeurs de a. Un nombre a ne vérifiant pas ce test pour n est appelé témoin de composition de n (ou témoin de Miller). Une propriété intéressante de ces témoins est qu'un nombre composé en possède toujours au moins un (ce qui évite le cas des nombres de Carmichael pour le test de Fermat), mais surtout : pour un nombre impair composé n, au moins 3/4 des entiers a, $1 < a < n$, sont des témoins de composition pour n.
2. Implémentez le test de Miller-Rabin.
   (a) Implémentez une fonction prenant deux arguments n et a et retournant `False` si a est un témoin de composition de n.
   (b) Implémentez un fonction prenant deux arguments n et k, répétant k fois le test précédent, pour des valeurs de a différentes.
   (c) Tester votre test de primalité sur les nombres inférieurs à 1000, et vérifier la véracité des résultats.