Institut Joseph Fourier
Master II C.S.C.I
2004-2005 - semaine 47

TP Maple - Théorie des Nombres.

TP2

Tests de primalité probabilistes

Sébastien Varrette `Sebastien.Varrette@imag.fr`
Gérard Vinel `Gerard.Vinel@ujf-grenoble.fr`

Conseils Préliminaires

Il vous est demandé de réaliser les exercices qui suivent sur une feuille de style Maple (format `.mws`). Cette dernière devra comporter outre les différentes procédures et quelques exemples pour les illustrer, les élements suivants :
– Titre du TP
– Noms des binômes
– Titre des exercices réalisés et justification des choix d'implémentation si besoin est.
– Tout commentaire qui vous paraît le bienvenu.
Pour chaque procédure vous sera précisé son prototype (variables d'entrée (Input), de sortie (Output) et les eventuelles contraintes sur ces paramètres). Merci de les rappeler et d'en tenir compte dans la réalisation pratique de ces procédures.
Cette feuille de style devra être envoyée par mail aux adresses mails ci-dessus.
TODO : voir éventuellement un autre mode de dépot

L'aide de Maple est très utile et pratique : utilisez la !
Enfin, n'oubliez pas de commenter et d'indenter votre code.

1 Legendre et Jacobi

1.1 (pour bien démarrer la journée) Symbole de Legendre

Soit $a \in \mathbb{Z}$ et p un nombre premier impair. Le symbole de Legendre $\left(\frac{a}{p}\right)$ est définit par :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } a \\ 1 & a \text{ est un carré modulo } p, \text{ ou } a \text{ est un résidu quadratique de } p \\ -1 & \text{sinon} \end{cases}$$

Le symbole de Legendre admet un certain nombre de propriétés qui sont listés ici :

$$\left(\frac{a}{p}\right) = a^{\left(\frac{p-1}{2}\right)} \mod p \quad (1)$$

$$\left(\frac{i}{p}\right) = i \text{ pour } i \in \{0,1\} \quad (2)$$

$$\left(\frac{-1}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)} \quad (3)$$

$$\left(\frac{a}{p}\right) = \left(\frac{a \mod p}{p}\right) \quad (4)$$

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \quad (5)$$

$$\left(\frac{2a}{p}\right) = \left(\frac{a}{p}\right)(-1)^{\left(\frac{p^2-1}{8}\right)} \quad (6)$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{(p-1)(q-1)}{4}\right)} \quad (7)$$

La dernière propriété s'appelle loi de réciprocité quadratique. La première propriété permet de calculer directement $\left(\frac{a}{p}\right)$ tandis que les propriétés suivantes permettent d'aboutir à une résolution récursive.

Exercice 1. *Réaliser la procédure* `SymbLegendre`.
Tester votre procédure sur quelques exemples.

Procedure `SymbLegendre(`a`,`p`)`

Input: $a \in \mathbb{Z}$, p un nombre premier

Output: $\left(\frac{a}{p}\right)$

1.2 (parce qu'il faut bien travailler) Symbole de Jacobi

On étend la définition du symbole de Legendre. Soit n un **entier impair**. Sa décomposition en facteurs s'écrit :

$$n = \prod_{i=1}^{k} p_i^{e^i}$$

Soit $a \geq 0$ Le symbole de jacobi $\left(\frac{a}{n}\right)$ est définit par :

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

En particulier, $\left(\frac{1}{n}\right) = 1$ et $\left(\frac{0}{n}\right) = 0$. Plusieurs règles permettent de calculer $\left(\frac{a}{n}\right)$ en temps polynomial sans factoriser n :

$$\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right) \text{ Si } m_1 \equiv m_2 \mod n \tag{8}$$

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{si } n \equiv \pm 1 \mod 8 \\ -1 & \text{si } n \equiv \pm 3 \mod 8 \end{cases} \tag{9}$$

$$\left(\frac{xy}{n}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \tag{10}$$

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{si } m \equiv n \equiv 3 \mod 4 \\ \left(\frac{n}{m}\right) & \text{sinon} \end{cases} \tag{11}$$

En particulier de (10), si $m = 2^s t$ avec t impair, alors $\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^s \left(\frac{t}{n}\right)$
(11) correspond à la loi de réciprocité généralisée et reste valable pour m entier impair.

Exercice 2. *Réaliser la procédure* `SymbJacobi` *sans avoir recours à la factorisation de n. Tester votre procédure sur quelques exemples.*

Procedure `SymbJacobi(a,n)`

Input: $a, n \in \mathbb{N}$, n entier impair

Output: $\left(\frac{a}{p}\right)$

---

2 Tests de primalité probabilistes

2.1 (le plus simple) Test de Fermat

Théorème 1 (Petit théorème de Fermat)**.** *Si n est premier alors* $\forall a \in \mathbb{Z}$ *tel que pgcd(a,n)=1,* $a^{n-1} \equiv 1 \mod n$

La réciproque de ce théorème est fausse ! (voir les nombres de Carmichaël).
mais on utilise la contraposée de ce théorème pour détecter les nombres qui ne sont pas premiers :
Si $\exists a \in \mathbb{Z}/pgcd(a,n) = 1$ ET $a^{n-1} \not\equiv 1 \mod n$, alors n n'est pas premier.
L'idée est donc de tirer au hasard un certain nombre de a tels que pgcd(a,n)=1 puis de calculer $a^{n-1} \mod n$ Si on obtient au moins une fois une valeur différente de 1, alors n est composé (et c'est sûr). En revanche, si on a obtenu que des 1, alors n est probablement premier (dans ce cas, on dit que n est pseudo-premier)

Exercice 3. *Réaliser la procédure* `isPrimeFermat`*. Tester votre procédure sur quelques exemples, en particulier sur le nombre 561. Comparer vos résultats à ceux de la fonction Maple* `isprime`*.*

Procedure `isPrimeFermat(`n`)`

Input: $n \in \mathbb{N}$, n entier impair

Output: $\begin{cases} true & \text{si } n \text{ est pseudo premier} \\ false & \text{si } n \text{ est composé} \end{cases}$

2.2 (pour ne pas gaspiller) Test de Solovay-Strassen

On utilise pour cela le symbole de Jacobi (voir §1.2) :

Théorème 2. *Si n est nombre premier impair, alors $\forall a \in \mathbb{Z}$,*

$$\left(\frac{a}{n}\right) = a^{\left(\frac{p-1}{2}\right)} \mod p$$

L'idée est donc de choisir un nombre a, de calculer séparement chaque membre et de les comparer. S'ils diffèrent, n est composé, sinon on réitère avec un nouveau a jusqu'à avoir fait m tours. La probabilité d'erreur de ce test après m tours est $\frac{\log n - 2}{\log n - 2 + 2^{m+1}}$.

Exercice 4. *Réaliser la procédure* `isPrimeSolovayStrassen`*. Vous utiliserez pour cela votre procédure* `SymbJacobi` *Tester votre procédure sur quelques exemples et comparer vos résultats à ceux de la fonction Maple* `isprime`*.*

Procedure `isPrimeSolovayStrassen(`n`)`

Input: $n \in \mathbb{N}$, n entier impair

Output: $\begin{cases} true & \text{si } n \text{ est pseudo premier} \\ false & \text{si } n \text{ est composé} \end{cases}$

2.3 (the best) Test de Miller-rabin

Le principe est le suivant :
Soit n un nombre premier impair. On pose $n - 1 = 2^s.t = |\mathbb{Z}/n\mathbb{Z}^*|$.
Soit $a \in [1, p]$ un nombre aléatoire Soit alors k l'ordre de a^t. Alors $k|2^s$ donc k est une puissance de 2 : $k = 2^r$.

1. si $r = 0$ alors $k = 1$ et $a^t = 1 \mod n$
2. sinon, $a^{t2^r} \equiv 1 \mod n$ et donc $a^{t2^{r-1}}$ est d'ordre 2. Or, puisque n est premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps dans lequel le seul élément d'ordre 2 est -1 (il y a deux racines au polynôme $X^2 - 1$ qui sont 1 (d'ordre 1) et -1 (d'ordre 2))

L'idée est donc de construire la suite $\{p_i = a^{k2^i}\}_{0 \leq i \leq s}$. Chaque terme p_i est le carré du précédent. On déduit de ce qui précède que deux cas, et deux seulement, sont possibles pour la suite des p_i lorsque n est premier :

1. $p_0 = a^t = 1$ et alors $\forall i > 0$, $p_i = 1$.
2. $\exists\ i < s\ /\ p_i = -1$ et dans ce cas, $\forall j > i$, $p_j = 1$

Si la suite des p_i ne vérifie aucune de ces deux conditions, n est composite ; si par contre elle vérifie l'une de ces deux conditions, n est vraisemblablement premier.

Exercice 5. *Réaliser la procédure* `isPrimeMillerRabin`*. Tester votre procédure sur quelques exemples (notamment 561) et comparer vos résultats à ceux de la fonction Maple* `isprime`*.*

Procedure `isPrimeMillerRabin`(n)

Input: $n \in \mathbb{N}$, n entier impair

Output: $\begin{cases} true & \text{si } n \text{ est pseudo premier} \\ false & \text{si } n \text{ est composé} \end{cases}$
