Algorithmique Algébrique

TD4 Exercice 9 (critère de Wilson).

Soit $n \geq 2$ un entier. Nous allons montrer que n est premier si et seulement si $(n-1)! \equiv -1[n]$.

1) Supposons que $n = ab$ avec $a > 1,\ b > 1$ et $a \neq b$. Ici $a \mid n$ et $b \mid n$ strictement, donc $a < n$ et $b < n$ (si $a = n$ alors $b = 1$ et si $b = n$ alors $a = 1$ ce qui est impossible). Par définition $(n-1)!$ est le produit de tout les nombres plus grand que 1 et inférieurs ou égaux à $n-1$, les nombres a et b font alors partie de ce produit donc $n = ab \mid (n-1)!$.
Une autre façon de le voir : $(n-1)! = (ab-1)! = (ab-1)(ab-2)\dots(ab-a)\dots(ab-b)\dots(3)(2)$ et $a \mid ab-a$ et $b \mid ab-b$, donc $n = ab \mid (n-1)!$.

Il est clair que si n est premier il ne peut exister une telle décomposition. Si n n'est pas premier alors n se décompose en produit de facteurs premiers. Il y a alors plusieurs cas :

1. Si un seul premier intervient dans la décomposition de n, autrement dit $n = p^\alpha$:
   (a) si $n = p^2$, on ne peut rien faire,
   (b) si $n = p^\alpha$ avec $\alpha > 2$, alors $n = ab$ avec $a = p$ et $b = p^{\alpha-1}$ et on a bien $a, b > 1$ et $a \neq b$ car $\alpha - 1 \neq 1$.
2. Si il existe au moins deux premiers distincts dans la décomposition de n, il est alors assez clair que n puisse s'écrire sous la forme $n = ab$ avec $a, b > 1$ et $a \neq b$.

Les n ne possédant pas une telle décomposition sont donc les nombres premiers et les carrés de nombre premiers.

2) Supposons que $n = p^2$, où p est un premier différent de 2. Alors $p < n$ et $2p < n$ (si $2p = n$ on aurait $p = 2$, impossible). Les nombres p et $2p$ interviennent donc dans le produit $(n-1)! = (n-1)(n-2)\dots(3)(2)$ donc $2p^2 \mid (n-1)!$ donc $n = p^2 \mid (n-1)!$.

Pour $p = 2$ on a $n = 4$ et $(4-1)! = 3! = 6$ et $6 \equiv 2[4]$.

3) Supposons que $n = p$, où p est un premier. Si a est tel que $a \not\equiv 0[p]$, p étant premier cela équivaut à ce que a soit premier à p. On sait dans ce cas que a possède un inverse modulo p (en effet a et p étant premier, il existe des entiers u et v tels que $au + pv = 1$, en passant cette expression modulo p on obtient qu'il existe un entier u tel que $au \equiv 1[p]$).

Un nombre a est sont propre inverse modulo p si et seulement si $a^2 \equiv 1[p]$ donc si et seulement si $p \mid a^2 - 1$. On a $(a^2-1) = (a+1)(a-1)$ donc si $p \mid (a^2-1)$ nécessairement $p \mid a+1$ ou $p \mid a-1$. En terme de congruence, $p \mid a+1 \iff a+1 \equiv 0[p] \iff a \equiv -1[p]$ et $p \mid a-1 \iff a \equiv 1[p]$. Un nombre a est donc son propre inverse si et seulement si $a \equiv \pm 1[p]$.

4) Toujours pour $n = p$ un premier, $(p-1)!$ est en effet le produit de tout les restes non nuls possible modulo p, puisque c'est exactement le produit de tout les nombres > 0 plus petit que $p-1$. On a vu par la question précédente que tout les nombres positifs plus petit que p sont inversibles modulo p (si x est compris entre 1 et $p-1$ il existe un nombre y, lui aussi compris entre 1 et $p-1$ tel que $xy \equiv 1[p]$), et que seul 1 et $p-1$ sont leurs propre inverse. Lorsque l'on

calcul $(p-1)!$ on fait le produit de tout les nombres compris entre 1 et $p-1$, pour chaque nombre intervenant dans ce produit, il va exister un inverse pour ce nombre modulo p qui lui aussi sera dans le produit. Dans le produit, tout les termes n'étant pas leurs propre inverse vont donc se télescoper, le produit $(p-1)!$ modulo p est donc égal à $1 \times (p-1) \equiv -1[p]$.

5) On a montré à la question précédente que si n est premier, alors $(n-1)! \equiv -1[n]$. Si n n'est pas premier, on a vu par la question 1) que n était deux formes possible :

1. Soit il est de la forme $n = ab$ avec $a, b > 1$ et $a \neq b$, et par la question 1) on a $(n-1)! \equiv 0[n]$.
2. Soit il est de la forme $n = p^2$ et par la question 2) :
   (a) si $p = 2$, on a $(n-1)! = 3! \equiv 2[4]$
   (b) si $p > 2$, on a $(n-1)! \equiv 0[n]$.

Dans tout les cas où n n'est pas premier, $(n-1)!$ n'est pas congru à -1 modulo p (en fait si n est pas premier, soit $n = 4$ et $(n-1)! \equiv 2[4]$, soit $(n-1)! \equiv 0[n]$). Ceci démontre l'équivalence.

6) On peut en déduire l'algorithme suivant pour n un entier :

1. On calcule $(n-1)!$,
2. On effectue la division euclidienne de $(n-1)!$ par n,
3. Le nombre n est premier si et seulement si le reste est $n-1$.

Cet algorithme est bien sûr extrêmement coûteux, le calcul de $(n-1)!$ est en $O(n^2 \log^2(n))$. Le coût de la division euclidienne est en $O(\log((n-1)!)\log(n)) = O(n \log^2(n))$ donc le coût de l'algorithme au total est en $O(n^2 \log^2(n))$.

Bonus : Essayons d'être plus fin, et d'effectuer les multiplications pour calculer $(n-1)!$ directement modulo n :

1. On pose $x = 1$
2. Pour i allant de 2 à $n-1$ on pose $x = x \times i\ [n]$:
   (a) on calcule $x \times i$,
   (b) on donne à x la valeur du reste de la division euclidienne de $x \times i$ par n.
3. Le nombre n est premier si et seulement si après l'étape précédente $x = n-1$.

Estimons la complexité de cet algorithme : on fait $(n-2)$ fois l'étape 2). L'avantage de cette méthode est qu'à chaque étape x est compris entre 1 et $n-1$. Le coût de la multiplication $x \times i$ est donc en $O(\log^2(n))$. Le coût de la division euclidienne est en $O(\log(n^2)\log(n)) = O(\log^2(n))$. Le coût d'une itération à l'étape 2) est donc en $O(\log^2(n))$ donc le coût de l'algorithme total est en $O((n-2)\log^2(n)) = O(n \log^2(n))$. C'est beaucoup mieux ! Mais ce n'est pas mieux que l'algorithme naïf consistant à faire la division euclidienne de n par tout les nombres plus petit que $\lfloor \sqrt{n} \rfloor$, qui lui est en $O(\sqrt{n} \log^2(n))$.
Le critère de Wilson est donc un résultat théorique intéressant mais qui ne fournit pas un critère efficace pour tester la primalité d'un nombre.