Les maths de l'algortihme de Maurer (provable primes) :

On souhaite prouver la correction de l'algorithme de Maurer, c'est à dire qu'il nous renvoie bien des premiers prouvables.
Nous devons premièrement donner quelques résultats utiles afin de le démontrer.

Définition 1 : L'ordre d'un élément g d'un groupe G est le plus petit m tel que $g^m \equiv e$, où e est l'élément neutre du groupe.
Nous travaillons dans le groupe $(Z/nZ)^*$, il en résulte donc que $g^m \equiv 1 \pmod n$

Théorème 2 : Si G est un groupe multiplicatif d'ordre n , et $g \in G$, alors l'ordre de g appelé m divise n. (Théorème de Lagrange).

Corollaire : Si $b \in (Z/nZ)^*$, alors $b^{\varphi(n)} \equiv 1 \pmod n$

Théorème 3 (Théorème de Lucas) : Soint $n > 1$, s'il existe un facteur premier q de n-1 tel que :
- $a^{n-1} \equiv 1 \pmod n$
- $a^{(n-1/q)} \not\equiv 1 \pmod n$

Alors n est premier.

Théorème 4 (Théorème de Pocklington) : Soit $n - 1 = q^k * R$ où q est un nombre premier tel que q ne divise pas R. S'il existe un entier a tel que :
- $a^{n-1} \equiv 1 \pmod n$
- $pgcd(a^{(n-1/q)} - 1, n) = 1$

Alors chaque facteur premier p de n est de la forme $p = (q^k)*r + 1$ où r est un entier.

Les Théorèmes 3 et 4 peuvent être prouvés assez rapidement en utilisant la Définition 1, ainsi que le Théorème 2 et le Corollaire.

Le Théorème 4 limite nos possibilités étant donné que seul les composés de la forme $q^k * R$ peuvent être prouvés. C'est pourquoi on doit étendre ce résultat au cas général où $n-1 = F * R$, avec $F > R$ et $pgcd(R,F) = 1$.

Théorème 5 : Soit $n-1 = F*R$, où $F>R$ (R est donc $< \sqrt{n}$), $pgcd(F,R) = 1$ et la factorisation p1,p2, …,pm de F est connue. Si pour tous les pi, il existe un $a > 1$ tel que :
- $a^{n-1} \equiv 1 \pmod n$

-$pgcd(a^{(n-1/pi)} - 1, n) = 1$
alors n est premier.

La preuve de ce théorème résulte directement de celle des théorèmes 3 et 4 en se rappelant que q ne divise pas R, il suffit maintenant de le montrer pour tous les facteurs de premiers de F.

Le théorème de Maurer se découpe donc en 2 phases, une qui utilise les divisons successives (pour $k<20$ pour k le nombre de bits du premier souhaité), l'autre qui utilise le Théorème 5.

Ainsi on obtient le certificat du nombre n généré par l'algorithme de Maurer : le triplet (R,F,a) ainsi que la factorisation de F où $n = 2RF + 1$.