Tests de primalité (Gourdon)

Pierre Lissy

April 9, 2010

Critère 1: ceci implique que l'ordre de a est $n-1$ dans l'ensemble des inversibles de Z/nZ. Autrement dit l'ensemble des inversibles est de cardinal au moins $n-1$ donc de cardinal $n-1$ et c'est nécessairement que n est premier.
Critère 2: Notons m_i l'ordre de a_i dans le groupe des inversibles de Z/nZ. d'après les hypothèses, on a $m_i|n-1$, avec $n-1=\prod p_i^{\alpha_i}$. mais $a_i^{(n-1)/p_i}$, on a aussi $m_i \not| p_i^{\alpha_i-}\prod_{j\neq i} p_j^{\alpha_j}$. On a donc que $p_i^{\alpha_i}|m_i$, et donc que $p_i^{\alpha_i}|\varphi(n)$, puisque l'ordre des inversibles de Z/nZ est $\varphi(n)$. Comme les p_i sont premiers entre eux distincts, leur produit, ie $n-1$, divise $\varphi(n)$. Donc $\varphi(n)=n-1$, ce qui implique par définition (n'a du coup aucun diviseur autre que 1) que n est premier.
Critère 3: c'est le plus intéressant. Soit m l'ordre de 2 dans le groupe des inversibles de Z_n. Comme $2^{n-1}\equiv 1[n]$, on a $m|n-1=hp^2$. Mais $2^h \not\equiv 1[n]$ donc $m \not| h$. Donc $p|m$ (sinon par le théorème deGauss, comme $m|hp^2$, cela veut dire que $m|h$ ce qui est faux par hypothèse). Or $m|\varphi(n)$ donc $p|\varphi(n)$. Posons $n=\prod p_i^{\alpha_i}$, alors $\varphi(n)=\prod p_i^{\alpha_i-1}(p_1-1)\dots(p_k-1)$. On dait que p ne divise pas n, donc p n'est pas égal à un p_i et donc $p=p_i-1$. Donc $p_i\equiv 1[p]$. On a $p_i r=n=1+hp^2\equiv 1[p]$, donc compte tenu que $p_i\equiv 1[p]$ on obtient $r\equiv 1[p]$. $p_i=1+up$ et $r=1+^v p$. Supposons $r>1$. Alors $v\geqslant 1$. On a $1+hp^2=(1+up)(1+vp)$ donc $hp=uvp+(u+v)$, ce qui entraine $uv<h\leqslant p-1$ et $(u+v)\geqslant p$ car $p|(u+v)$. Comme $u\geqslant 2$, on a $v<(p-1)/2$ et donc $u\geqslant 1+p/2$, et donc $v<(p-1)/(1+p/2)<2$. Finalement $v=1$, ce qui est absurde car on aurait $u<p-1$ et donc $e\geqslant u-1$ aussi... Finalemenr $r=1$, et donc $n=q$ est premier.

Exemple 1. *$n=1+hp^2$ premier, avec $h=190$ et $p=2^{127}-1$. En effet, on admet que p premier, et on tente de voir ce que donne 2^190. On a $p^2=2^{254}+1-2^{128}$ donc $n=1+190*(2^{254}+1-2^{128})>2^{254}-2^{128}=2^{128}(2^{126}-1)>2^{253}$. Donc clairement on ne peut avoir $2^{190}\equiv 1[n]$. reste à voir si $2^{n-1}\equiv 1[n]$. On l'admet.*