Facteurs carrés des nombres de Mersenne

blogdemaths.wordpress.com

Dans ce document, on montre que si un nombre de Mersenne 2^q-1 avec q premier possède un facteur carré, alors il est divisible par un nombre premier de Wieferich.

Commençons par donner la forme des diviseurs premiers des nombres de Mersenne 2^q-1 :

Proposition. Soit $p>2$ et $q>2$ deux nombres premiers. Si p divise 2^q-1 alors il est de la forme

$$p=2kq+1 (k\in\mathbb{N})$$

Démonstration. Comme p divise 2^q-1 alors $2^q\equiv 1 \mod [p]$. Ainsi, l'ordre de 2 modulo p divise q. Comme q est un nombre premier, l'ordre de 2 vaut donc soit 1, soit q. Comme $2^1\not\equiv 1 \mod [p]$, c'est que l'ordre de 2 est égal à q.
Or, 2 est premier avec p donc d'après le petit théorème de Fermat,

$$2^{p-1}\equiv 1 \mod [p]$$

Ainsi, l'ordre de 2 divise $p-1$. Par suite, q divise $p-1$ donc il existe un entier k' tel que $p-1=k'q$ c'est-à-dire $p=k'q+1$.
Enfin, k' ne peut être impair car sinon $k'q+1$ serait un nombre pair. Ainsi, il existe un entier k tel que $k'=2k$ ce qui donne $p=2kq+1$. □

Définition. Soit p un nombre premier. On dit que p est un nombre premier de Wieferich si p^2 divise $2^{p-1}-1$.

Proposition. Soit q un nombre premier. Si 2^q-1 est divisible par p^2 où p est un nombre premier, alors p est un nombre premier de Wieferich.

Démonstration. On suppose que 2^q-1 est divisible par p^2 où p est un nombre premier. En particulier, 2^q-1 est divisible par p donc on sait que p est de la forme $p=2kq+1$ $(k\in\mathbb{N})$ ce qui donne $q=\frac{p-1}{2k}$. De la relation $2^q\equiv 1 \mod [p^2]$, on obtient

$$2^{\frac{p-1}{2k}}\equiv 1 \mod [p^2]$$

En prenant cette relation à la puissance $2k$ des deux côtés, on a alors $2^{p-1}\equiv 1 \mod [p^2]$, ce qui veut bien dire que p est un nombre premier de Wieferich. □