

Pierre Lissy

April 24, 2010

Lemme 1. *Les facteurs premiers de $\Phi_a(n)$ (pour n non égal à 0,1,-1) sont soit ceux de a , soit de la forme $ak + 1$.*

Proof. On sait que les polynômes cyclotomiques sont à coefficients entiers. Donc comme $\mathbb{Z}$ est un anneau on a déjà $\Phi(n) \in \mathbb{Z}$. De plus, on a $|\varphi(n)| \geq 2$ par l'inégalité suivante que je vais prouver:

Lemme 2. *Pour tout réel $|x| > 1$, on a $|\Phi(x)|(|x| - 1)^{\varphi(n)}$.*

Proof. $\Phi_n(x) = \prod (x - \xi_i)$ où les ξ_i sont les racines n -ièmes de l'unité. Or un dessin montre à peu près trivialement que $|x - \xi_i| > 1$ dans le cas qui nous intéresse. $\square$

On a donc bien ce qu'on voulait. $\Phi_a(n) = n^{\varphi(n)} + \dots + 1$. Soit p un facteur premier de $\Phi_a(n)$, dans $\mathbb{Z}/p\mathbb{Z}$ on a $\Phi_a(n) = 0$ donc compte tenu de la relation $X^a - 1 = \prod_{d|a} \Phi_d(X)$, n est racine de $X^a - 1$. On a donc que n vérifie dans $\mathbb{Z}/p\mathbb{Z}^*$ que $n^a = 1$. Si on suppose que p ne divise pas a , alors on a que n est une racine simple du polynôme. Soit s l'ordre de n . Si on supposait $s < a$, on aurait $a^s = 1$ et donc, comme $X^a - 1 = (X^k - 1)\Phi_a(X)R(X)$, ce la signifierait que n serait racine multiple de $X^a - 1$ ce qui est faux. Ainsi $s = a$ et nécessairement par le théorème de Lagrange que a divise $p - 1$. Comme annoncé, $ak + 1 = p$. $\square$

On en déduit maintenant le théorème. On note $F = \{q_1, \dots, q_m\}$ l'ensemble des facteurs premiers de a . Supposons que l'ensemble E des nombres premiers de la forme $ak + 1$ soit fini, d'éléments $p_1, \dots, p_s$. Considérons $n = q_1 \dots q_m p_1 \dots p_s$. D'après le sous-lemme précédent, on a $|\Phi_a(n)| \geq 2$. De plus, $\Phi(n) = n^{\varphi(n)} + \dots + 1$ donc $\varphi_a(n)$ est congru à 1 modulo les p_i et les q_j . Soit q un facteur premier de $\varphi_a(n)$, par définition, on a $\varphi_a(n) \equiv 0[q]$, donc $q \notin E$ et $q \notin F$ au vu de ce qu'on a dit précédemment. Mais d'après le lemme 1 on devrait avoir soit q qui divise a , soit q de la forme $ak + 1$, autrement dit $q \in E$ ou $Q \in F$. On obtient bien une contradiction.

References

[1]