Algorithmique Algébrique

TD3 Exercice 5.

Montrons qu'il existe une infinité de nombre premier de la forme $4k+3$ pour $k \in \mathbb{N}$. Supposons par l'absurde qu'il en existe un nombre fini $p_1, p_2, \ldots, p_n$, posons :

$$p = 4 \times \left(\prod_{i=1}^{n} p_i \right) - 1, \text{ avec } \; p_i = 4k_i + 3.$$

Montrons que si p n'est pas premier il existe au moins un premier p_j qui divise p. Le nombre p se décompose en facteur premier, comme p est impair les seuls premiers intervenant dans la décomposition en facteur premier sont soit de la forme $4k+3$ soit de la forme $4k+1$ (en fait, tout nombre impair s'écrit sous l'une de ces deux formes car si un nombre est de la forme $4k$ ou de la forme $4k+2$, il est nécessairement pair). Le nombre p est donc un produit de nombres premiers de la forme $4k+3$ ou $4k+1$. Supposons par l'absurde que les facteurs de p soient tous de la forme $4k+1$, alors p lui même devrait être de la forme $4k+1$. En effet un produit de nombres de la forme $4k+1$ est encore de la forme $4k+1$:

$$(4a+1) \times (4b+1) = 16ab + 4(a+b) + 1 = 4(4ab + a + b) + 1.$$

Le nombre p serait alors de la forme $4k+1$, ce qui est absurde puisqu'il est de la forme $4k-1$ (le reste dans la division euclidienne par 4 est différent). Il existe donc au moins un facteur premier de p de la forme $4k+3$, autrement dit il existe un p_j tel que $p_j \mid p$.

Le nombre p_j divise p et $\prod_i p_i$ donc devrait diviser -1, ce qui est impossible. Ceci montre donc que p est premier. Or $p = 4\big(\prod_i p_i\big) - 1 = 4\big(\prod_i p_i - 1\big) + 3$ et est donc un premier de la forme $4k+3$ qui ne fait clairement pas partie des p_i. Il était donc absurde de supposer qu'il existe un nombre fini de nombre de la forme $4k+3$, en conclusion il en existe alors une infinité.