Nombres de Fermat

Ayoub Hajlaoui

Élève batailleur, la balle est dans ton camp :
Gardons un dur labeur au milieu du boucan.

Cet exercice demande des pré-requis de Terminale S spé maths.

Énoncé : (temps conseillé : 25 min)

Pour tout entier naturel k, on note F_k le nombre de Fermat $F_k = 2^{2^k} + 1$.
Soient m et n deux entiers naturels tels que $n \neq m$.
Montrer que F_m et F_n sont premiers entre eux.

Correction :

Deux entiers premiers entre eux sont deux entiers dont le PCGD est 1. *Il est donc judicieux d'introduire le PGCD de F_m et F_n.*

Soit d le PGCD de F_m et F_n.
F_m et F_n sont des multiples de d (puisque d est un diviseur de F_m et F_n, et plus spécifiquement le plus grand). Donc $F_n \equiv 0\ [d]$ et $F_m \equiv 0\ [d]$

On aurait pu être plus précis en posant $F_n = d\alpha_n$ et $F_m = d\alpha_m$ avec α_n et α_n premiers entre eux. En l'occurrence, ici, on n'en aura pas besoin, mais c'est bon de l'avoir en tête.

Donc $2^{2^n} + 1 \equiv 0\ [d]$ et $2^{2^m} + 1 \equiv 0\ [d]$

Donc $2^{2^n} \equiv -1\ [d]$ et $2^{2^m} \equiv -1\ [d]$

Que faire, maintenant ? Quel lien y a-t-il entre 2^{2^m} et 2^{2^n} ?

Par hypothèse, $n \neq m$. Sans perte de généralité, prenons donc $n > m$.
Sans perte de généralité, puisque le cas $m < n$ est obtenu en intervertissant simplement m et n dans le raisonnement.

Dès lors, $2^n = 2^m \times 2^{n-m}$ et donc $2^{2^n} = 2^{2^m \times 2^{n-m}} = (2^{2^m})^{2^{n-m}}$ avec 2^{n-m} entier puisque $n > m$
N'hésitez pas à zoomer, les puissances de puissance de puissance, ça fait mal aux yeux...

Comme $2^{2^m} \equiv -1\ [d]$, on a alors $2^{2^n} \equiv (-1)^{2^{n-m}}\ [d]$. *En quoi est-ce intéressant ? Que dire de l'exposant 2^{n-m} ?*
L'entier 2^{n-m} est une puissance de 2 avec $n - m > 0$. Il est donc pair *(la seule puissance de* 2 *impaire étant* $2^0 = 1$*)*. Donc $(-1)^{2^{n-m}} = 1$. On a donc en fait : $2^{2^n} \equiv 1\ [d]$.
On avait montré aussi précédemment $2^{2^n} \equiv -1\ [d]$.
Donc $1 \equiv -1\ [d]$.

www.ayoub-et-les-maths.com
ayoub.hajlaoui.scolaire@gmail.com

En effet, nous savons que si $a \equiv b\ [d]$ et $a \equiv c\ [d]$, alors $b \equiv c\ [d]$. Autrement dit, la relation de congruence modulo d est une relation transitive. Ajoutons, pour l'anecdote (et surtout pour la rentrée prochaine), que c'est aussi une relation réflexive ($a \equiv a\ [d]$) et symétrique (si $a \equiv b\ [d]$, alors $b \equiv a\ [d]$). Ces trois propriétés lui donnent le caractère de relation d'équivalence.

$1 \equiv -1\ [d]$ peut se traduire ainsi : il existe $k \in \mathbb{Z}$ tel que $1 = kd - 1$.
Autrement dit, il existe $k \in \mathbb{Z}$ tel que $kd = 2$.
Donc d divise 2.

Vous connaissez beaucoup d'entiers naturels qui divisent 2 ?

Donc $d = 1$ ou $d = 2$.

Nous cherchons à montrer $d = 1$. Cherchons donc ce qui l'empêche d'être égal à 2...

F_m et F_n sont tous les deux impairs $(F_k = 2^{2^k} + 1)$
Donc d (qui les divise) ne peut pas être égal à 2.
Donc $d = 1$.
Donc le PGCD de F_m et F_n est égal à 1.

Donc F_m et F_n sont premiers entre eux.

www.ayoub-et-les-maths.com
ayoub.hajlaoui.scolaire@gmail.com