Un nombre de Fermat non premier

Ayoub Hajlaoui

D'observations tronquées, la fausse idée germa :
Mes nombres sont premiers, conjectura Fermat.

Énoncé : (temps conseillé : 30 min)

Pour tout entier naturel n, on pose $F_n = 2^{2^n} + 1$. Les F_n sont appelés nombres de Fermat.
1) Vérifier que F_0, F_1, F_2 et F_3 sont premiers.
2) On veut montrer que F_5 n'est pas premier. (*Remarquons :* $641 = 2^4 + 5^4 = 5 \times 2^7 + 1$)
a) Montrer que 641 divise $2^{32} + 5^4 \times 2^{28}$
b) Montrer que 641 divise $5^4 \times 2^{28} - 1$
c) En déduire que 641 divise F_5. Conclure.

Correction :

1) *Rappelons qu'un nombre premier est un nombre divisible uniquement par* 1 *et par lui-même,* 1 *et lui-même devant être distincts (*1 *n'est donc pas premier).*
$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 2 + 1 = 3$ et 3 est bien premier.
$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5$ et 5 est bien premier.
$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$ et 17 est bien premier.

$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257$.
Astuce/rappel : pour savoir si un nombre N est premier, on regarde s'il est divisible ou pas par un nombre premier inférieur ou égal à $\sqrt{N}$ (en effet, tous les diviseurs de N autres que N lui-même sont inférieurs ou égaux à $\sqrt{N}$).
$16 < \sqrt{257} < 17$. Il suffit donc de voir si F_3 est divisible par 2, 3, 5, 7, 11 ou 13.
257 n'est évidemment pas pair, donc pas divisible par 2.
$2 + 5 + 7 = 14$ non divisible par 3, donc 257 n'est pas divisible par 3.
257 ne se termine ni par 0 ni par 5, donc 257 n'est pas divisible par 5.
Enfin, on vérifie que 257 n'est divisible ni par 7, ni par 11, ni par 13.
F_3 est bien premier.

En conclusion, pour tout n compris entre 0 et 3, F_n est premier.

2)a) $2^{32} + 5^4 \times 2^{28} = 2^{28} \times 2^4 + 5^4 \times 2^{28} = 2^{28} \times (2^4 + 5^4) = 2^{28} \times 641$ qui est un multiple de 641.
Donc 641 divise $2^{32} + 5^4 \times 2^{28}$

2)b) $5^4 \times 2^{28} - 1 = 5^4 \times (2^7)^4 - 1 = (5 \times 2^7)^4 - 1 = (5 \times 2^7)^4 - 1 = \left((5 \times 2^7)^2\right)^2 - 1^2$
Donc (3ème identité remarquable) $5^4 \times 2^{28} - 1 = \left[(5 \times 2^7)^2 + 1\right]\left[(5 \times 2^7)^2 - 1\right]$
En réutilisant cette même identité remarquable dans le second crochet, on obtient :
$5^4 \times 2^{28} - 1 = \left[(5 \times 2^7)^2 + 1\right](5 \times 2^7 + 1)(5 \times 2^7 - 1) = \left[(5 \times 2^7)^2 + 1\right] \times 641 \times (5 \times 2^7 - 1)$
Finalement, $5^4 \times 2^{28} - 1 = 641 \times \left[(5 \times 2^7)^2 + 1\right](5 \times 2^7 - 1)$ qui est un multiple de 641.
641 divise donc $5^4 \times 2^{28} - 1$.

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

2)c) $F_5 = 2^{2^5} + 1 = 2^{32} + 1$

Il faut garder en tête ce qui a été fait. En 2)a), on a montré que 641 *était divisible par un certain nombre. En 2)b), on a montré que* 641 *était divisible par un autre nombre. Et dans cette question-ci, on veut montrer que* 641 *divise un troisième nombre... On pense donc tout naturellement à la propriété suivante : " si* a *divise* b *et si* a *divise* c*, alors* a *divise toute combinaison linéaire de* b *et* c*. "*

Et si on essayait d'écrire F_5 *comme combinaison linéaire de* $2^{32} + 5^4 \times 2^{28}$ *et* $5^4 \times 2^{28} - 1$ *?*

$F_5 = 2^{32} + 1 = 2^{32} + 5^4 \times 2^{28} - 5^4 \times 2^{28} + 1$
(je fais apparaître le terme qui m'arrange et je compense ensuite en ajoutant son opposé)

Donc $F_5 = 2^{32} + 5^4 \times 2^{28} - (5^4 \times 2^{28} - 1)$
Or, d'après 2)a), 641 divise $2^{32} + 5^4 \times 2^{28}$ et d'après 2)b), 641 divise $5^4 \times 2^{28} - 1$.
641 divise donc toute combinaison linéaire de $2^{32} + 5^4 \times 2^{28}$ et $5^4 \times 2^{28} - 1$.
Finalement, 641 divise F_5.
641 est un diviseur de F_5 différent de 1 et de F_5
Ceci nous permet de conclure que F_5 n'est pas premier.