Maths Expertes
Terminale

Nombres Premiers

CORRIGÉ DE L'EXERCICE

Nombres premiers

08

Correction

1. Vérifions l'identité $x^k + 1 = (x+1) \times \left(x^{k-1} - x^{k-2} + \cdots - x + 1\right)$:

NB. L'entier k est par hypothèse un entier impair strictement plus grand que 1. La somme du deuxième facteur alterne les signes plus et moins.

Les termes d'exposants pairs sont affectés du signe plus (le premier d'entre eux étant celui d'exposant $(k-1)$ qui est un entier pair, le dernier est celui d'exposant zéro) et ceux d'exposant impairs du signe moins (le premier d'entre eux étant celui d'exposant $(k-2)$ qui est un entier impair, le dernier est celui d'exposant 1).

Considérons pour tout réel x le produit $P(x) = (x+1) \times \left(x^{k-1} - x^{k-2} + \cdots - x + 1\right)$ et développons-le en utilisant la distributivité de la multiplication sur l'addition :

$P(x) = (x+1) \times x^{k-1} - (x+1) \times x^{k-2} + \cdots + (x+1) \times x^2 - (x+1) \times x + (x+1)$ soit :
$P(x) = \left(x^k + x^{k-1}\right) - \left(x^{k-1} + x^{k-2}\right) + \cdots + (x^3 + x^2) - (x^2 + x) + (x+1)$.

Utilisons maintenant l'associativité de l'addition :
$P(x) = x^k + \left(x^{k-1} - x^{k-1}\right) - \left(x^{k-2} - x^{k-2}\right) + \cdots + (x^2 - x^2) - (x - x) + 1$.

Les termes x^j intermédiaires d'exposant j compris entre 1 et $k-1$ s'éliminent. Il nous reste, conformément à ce que nous attendions : $P(x) = x^k + 1$.

Nous avons bien vérifié que pour tout réel x : $x^k + 1 = (x+1) \times \left(x^{k-1} - x^{k-2} + \cdots - x + 1\right)$.

2. Déduisons-en que $2^{k\times 2^n}+1$ n'est pas un nombre premier :

Comme l'énoncé nous y invite, écrivons l'identité précédente en prenant pour valeur numérique la valeur $x=2^{2^n}$. Nous obtenons :

$$\left(2^{2^n}\right)^k+1=\left(2^{2^n}+1\right)\times\left(\left(2^{2^n}\right)^{k-1}-\left(2^{2^n}\right)^{k-2}+\cdots-\left(2^{2^n}\right)+1\right)$$

Compte tenu des règles de calcul sur les puissances, cette égalité s'écrit :

$$2^{k\times 2^n}+1=\left(2^{2^n}+1\right)\times\left(2^{(k-1)\times 2^n}-2^{(k-2)\times 2^n}+\cdots-2^{2^n}+1\right)$$

Le nombre entier $2^{k\times 2^n}+1$ se présente comme un produit de deux facteurs.

Montrons que $2^{2^n}+1$ en est un diviseur strict.

- D'une part pour tout entier naturel n : $2^{2^n}\geq 2^{2^0}=2$.
- D'autre part, le nombre k étant un nombre impair strictement plus grand que 1, il est au moins égal à 3, donc $k\times 2^n\geq 3\times 2^n>2^n$. il en résulte que $2^{k\times 2^n}>2^{2^n}$ (inégalité stricte) donc que : $2^{k\times 2^n}+1>2^{2^n}+1$.

Ainsi nous obtenons la double inégalité stricte : $2^{k\times 2^n}+1>2^{2^n}+1>1$.

Le nombre entier $2^{2^n}+1$ est un diviseur strict de $2^{k\times 2^n}+1$.

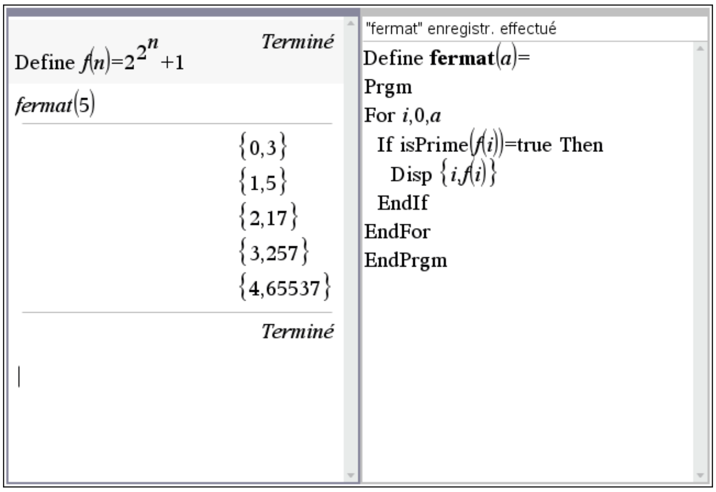
En conséquence, $2^{k\times 2^n}+1$ n'est pas un nombre premier.

NB. Pour exemple, sur cette copie d'écran de calculatrice, nous avons factorisé quelques nombres $2^{k\times 2^n}+1$.

Nous observons une factorisation par 17 lorsque $n=2$ et une factorisation par 257 lorsque $n=3$.

Define $g(n,k)=2^{k\cdot 2^n}+1$	*Terminé*
$g(2,3)$	4097
factor$(g(2,3))$	$17\cdot 241$
$g(2,5)$	1048577
factor$(g(2,5))$	$17\cdot 61681$
$g(3,3)$	16777217
factor$(g(3,3))$	$97\cdot 257\cdot 673$
$g(3,5)$	1099511627777
factor$(g(3,5))$	$257\cdot 4278255361$

3. Trouvons des nombres premiers dans la famille des $2^{k\times 2^n}+1$:

La question précédente nous montre que si $k > 1$, alors tous les nombres de la famille des $2^{k\times 2^n}+1$ sont des nombres composés. Il nous reste à tenter notre chance avec la seule valeur impaire non concernée, $k=1$, ce que nous faisons ci-contre. Bingo ! Nous trouvons 5 nombres premiers et, qui sait, il y en a peut-être d'autres (?).	

Si nous voulons trouver des nombres premiers dans la famille des $2^{k\times 2^n}+1$, il nous faut prendre la valeur $k=1$. Ainsi par exemple, $2^2+1=5$, $2^4+1=17$, $2^8+1=257$ sont bien des nombres premiers.

NB. Ces nombres sont connus comme étant les « nombres de Fermat » (voir article Wikipédia à leur propos). C'est pourquoi l'algorithme que nous avons utilisé pour aller à la pêche aux nombres premiers a été nommé « **fermat** ».