Maths Expertes
Terminale

Nombres Premiers

CORRIGÉ DE L'EXERCICE

Amusons-nous 02

Correction

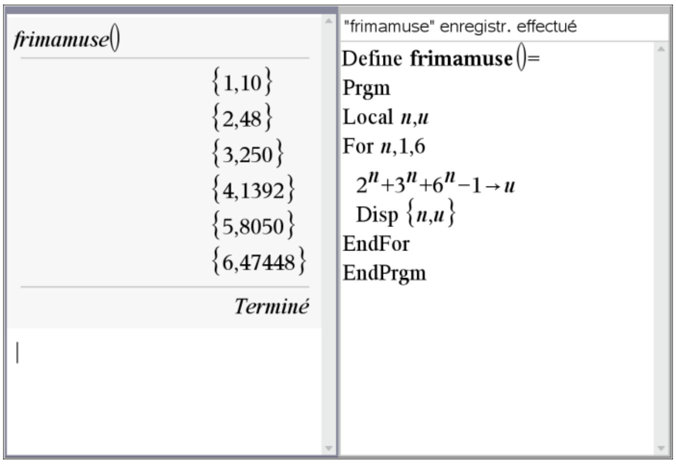
Dans cet exercice, la suite (u_n) est définie explicitement par : $u_n = 2^n + 3^n + 6^n - 1$. Cette suite possède une « propriété amusante ».

Rappelons, pour la résolution des **questions 5 et 6**, l'énoncé du petit théorème de Fermat :

Si P est un nombre premier et si a est un entier naturel non divisible par P, alors $a^{P-1} \equiv 1 \quad [P]$.

1. Calculons les six premiers termes de la suite :

Pour cela, aidons-nous d'une calculatrice. Nous faisons afficher l'indice n et le terme u_n pour n allant de 1 à 6.



2. Montrons que u_n est pair :

Pour tout entier n strictement positif : $u_n = (2^n + 6^n) + (3^n - 1)$.

- Le nombre $(2^n + 6^n)$ est pair car somme de deux nombres pairs. En effet, l'exposant n étant un entier strictement positif, les deux nombres 2^n et 6^n sont des entiers pairs.
- En revanche, 3^n est impair. Le nombre $(3^n - 1)$ est pair car différence de deux nombres impairs.

u_n est pair car il est la somme des deux nombres pairs $(2^n + 6^n)$ et $(3^n - 1)$.

3. Montrons que pour tout indice *n* pair, u_n est divisible par 4 :

Soit *n* un entier pair et strictement positif. Posons $n = 2p$ avec *p* strictement positif.

$$u_n = u_{2p} = 2^{2p} + 3^{2p} + 6^{2p} - 1$$

Utilisons des congruences modulo 4 :

- $2^2 = 4 \equiv 0 \quad [4]$, congruence qui implique, par élévation à la puissance *p*, la congruence $(2^2)^p = 2^{2p} \equiv 0^p \quad [4]$.
- $6^2 = 36 = 9 \times 4 \equiv 0 \ \ [4]$, congruence qui implique, par élévation à la puissance *p*, la congruence $(6^2)^p = 6^{2p} \equiv 0^p \ \ [4]$.
- $3^2 = 9 = 2 \times 4 + 1 \equiv 1 \ \ [4]$, , congruence qui implique, par élévation à la puissance *p*, la congruence $(3^2)^p = 3^{2p} \equiv 1^p \ \ [4]$.

Or, pour tout entier *p* strictement positif, $0^p = 0$ et $1^p = 1$.

(NB. Une nuance importante : 1 est invariant par élévation à une puissance entière relative (c'est l'élément neutre multiplicatif) tandis que 0 est invariant par élévation à une puissance entière strictement positive. L'hypothèse *n* entier pair strictement positif joue ici un rôle.)

Des trois congruences $2^{2p} \equiv 0 \quad [4]$, $\ 6^{2p} \equiv 0 \ \ [4]$ et $3^{2p} \equiv 1 \ \ [4]$, nous déduisons, par compatibilité de la relation de congruence modulo 4 avec l'addition que : $2^{2p} + 3^{2p} + 6^{2p} - 1 \equiv 0 + 1 + 0 - 1 \ \ [4]$ soit $2^{2p} + 3^{2p} + 6^{2p} - 1 \equiv 0 \ \ [4]$

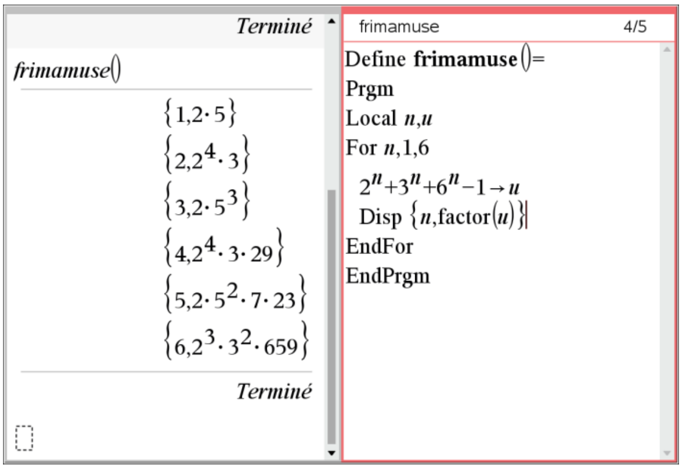
Pour tout entier *p* strictement positif, $u_{2p} \equiv 0 \ \ [4]$.

Nous avions posé $n = 2p$. Cette congruence modulo 4 exprime que :

Pour tout entier *n* pair et strictement positif, u_n est un multiple de 4.

4. Montrons que 2, 3, 5 et 7 appartiennent à *E* :

Modifions l'algorithme précédent en faisant afficher la version décomposée en produit de facteurs premiers des termes u_n. Nous relevons la présence du facteur 2 dans toutes les décompositions, du facteur 3 dans la décomposition de u_2, du facteur 5 dans celle de u_1 et du facteur 7 dans celle de u_5.



En conséquence, 2, 3, 5 et 7 appartiennent à *E*.

5.a. Montrons les congruences : $6 \times 2^{p-2} \equiv 3 \;\; [p]$ et $6 \times 3^{p-2} \equiv 2 \;\; [p]$:

NB. L'entier *p* est dans toute cette **question 5** et dans la **question 6** un nombre premier strictement supérieur à 3.

Remarquons que : $6 \times 2^{p-2} = 3 \times 2 \times 2^{p-2} = 3 \times 2^{p-1}$.

Remarquons aussi que : $6 \times 3^{p-2} = 2 \times 3 \times 3^{p-2} = 2 \times 3^{p-1}$

- Le nombre *p* est un nombre premier.
- Puisqu'il est > 3, *p* ne divise ni 2 ni 3.

Nous pouvons appliquer le petit théorème de Fermat avec le nombre premier *p* et avec $a = 2$.

Nous obtenons : $2^{p-1} \equiv 1 \;\; [p]$ d'où nous déduisons : $3 \times 2^{p-1} \equiv 3 \;\; [p]$.

Nous avons démontré : $6 \times 2^{p-2} \equiv 3 \;\; [p]$.

Appliquons-le aussi avec $a = 3$.

Nous obtenons : $3^{p-1} \equiv 1 \;\; [p]$ d'où nous déduisons : $2 \times 3^{p-1} \equiv 2 \;\; [p]$

Nous avons démontré : $6 \times 3^{p-2} \equiv 2 \;\; [p]$.

5.b. Déduisons-en la congruence $6u_{p-2} \equiv 0 \;\; [p]$:

Par définition de la suite (u_n) : $u_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$ et donc :

$$6u_{p-2} = 6 \times 2^{p-2} + 6 \times 3^{p-2} + 6^{p-1} - 6$$

Appliquons à cette égalité une congruence modulo *p* : $6u_{p-2} \equiv 6 \times 2^{p-2} + 6 \times 3^{p-2} + 6^{p-1} - 6 \;\; [p]$

Compte tenu des congruences vues dans la **question 5.a** : $6u_{p-2} \equiv 3 + 2 + 6^{p-1} - 6 \;\; [p]$,

Autrement dit : $6u_{p-2} \equiv 6^{p-1} - 1 \;\; [p]$.

Nous pouvons à cet instant songer à utiliser le petit théorème de Fermat.

- Le nombre *p* est un nombre premier.
- Le nombre premier *p* étant > 3, il est premier avec 2 et avec 3 donc avec leur produit 2×3 : les entiers 6 et *p* sont premiers entre eux, 6 n'est pas divisible par *p*.

Appliquons le petit théorème de Fermat avec $a = 6$.

Nous obtenons : $6^{p-1} \equiv 1 \;\; [p]$ d'où nous déduisons : $6^{p-1} - 1 \equiv 0 \;\; [p]$.

Par transitivité : $6u_{p-2} \equiv 0 \;\; [p]$.

6. Examinons si, oui ou non, le nombre premier *p* appartient à E :

La congruence $6u_{p-2} \equiv 0 \ [p]$ démontrée à la question 5.b montre que *p* divise $6u_{p-2}$.

Puisque 6 et *p* sont premiers entre eux, d'après le théorème de Gauss, *p* divisant le produit $6u_{p-2}$ et étant premier avec 6 : *p* divise u_{p-2}.

Quel qu'il soit, tout nombre premier *p* strictement supérieur à 3 divise le terme de la suite (u_n) de rang $p - 2$. Il appartient à *E*.

La copie d'écran ci-contre illustre, pour quelques-uns d'entre eux, le fait qu'un nombre premier $p > 3$ divise u_{p-2}.

Define $u(n)=2^n+3^n+6^n-1$	*Terminé*
$\frac{u(3)}{5}$	50
$\frac{u(5)}{7}$	1150
$\frac{u(9)}{11}$	917990
$\frac{u(11)}{13}$	27921250
$\frac{u(15)}{17}$	27658786250

Les questions précédentes ont montré que 2 et 3 appartenaient eux aussi à *E*. L'ensemble E n'est autre que l'ensemble de tous les nombres premiers.

La suite (u_n) possède la propriété suivante :

Chacun des nombres premiers, quel qu'il soit, apparait dans la décomposition en produit de facteurs premiers d'au moins un terme de la suite.