Maths Expertes
Terminale

Nombres Premiers

CORRIGÉ DE L'EXERCICE

Nombres premiers

01

Correction

NB. Soit *a* et *b* deux entiers. Rappelons que les formulations : « *a* est un multiple de *b* », « *b* divise *a* » et « *a* est divisible par *b* » sont équivalentes.

Partie A

Dans cette partie, *P* est un nombre premier au moins égal à 5.

1. Montrons que le nombre $A = (P^2 - 1)$ est divisible par 3 et par 8 :

NB. Nous aurons besoin dans notre démonstration de deux théorèmes que nous rappelons (justifications en note de bas de page) :

- T1. Etant donné trois nombres entiers consécutifs $n-1, n, n+1$, exactement l'un d'entre eux[1] est un multiple de 3.
- T2. Etant donné deux nombres pairs consécutifs $2p$ et $2p+2$, exactement l'un des deux[2] est un multiple de 4.

Le nombre $A = (P^2 - 1)$ est une différence de deux carrés et admet une factorisation :

$$A = (P-1) \times (P+1)$$

A est ainsi le produit des deux nombres entiers situés de part et d'autre du nombre *P* dans la file numérique.

[1] Etant consécutifs, ils sont congrus, modulo 3, aux entiers 0, 1 et 2, (respectivement soit dans l'ordre 2, 0, 1, soit dans l'ordre 0, 1, 2, soit dans l'ordre 1, 2, 0 suivant que *n* est congru à 0 ou à 1 ou à 2 modulo 3). Quel que soit le cas de figure, l'un d'eux, et un seulement, est congru à 0 modulo 3 donc est un multiple de 3.

[2] Si p est pair, il existe un entier q tel que $p = 2q$. Alors $2p = 4q$ donc $2p \equiv 0\ [4]$ et $2p + 2 = 4q + 2$ donc $2p + 2 \equiv 2\ [4]$. Si p est impair, il existe un entier q tel que $p = 2q + 1$. Alors $2p = 4q + 2$ donc $2p \equiv 2\ [4]$. Alors $2p + 2 = 4q + 4 = 4(q+1)$ donc $2p + 2 \equiv 0\ [4]$.
Quelles que soient les circonstances, exactement un des deux nombres, $2p$ ou bien $2p+2$, est congru à 0 modulo 4, donc est un multiple de 4.

Montrons que *A* est divisible par 3 :

Par hypothèse, en tant que nombre premier au moins égal à 5, *P* est distinct de 3. En tant que nombre premier distinct de 3, il est premier avec 3 et n'est pas multiple de 3.

D'après le théorème T1, l'un des trois entiers consécutifs $P-1, P, P+1$ est un multiple de 3. Ce multiple de 3 n'est pas l'entier *P*, c'est donc l'un des deux autres, ou bien $P-1$ ou bien $P+1$. Puisque l'un de ces deux nombres est un multiple de 3, leur produit $A = (P-1) \times (P+1)$ est aussi un multiple de 3.

$A = (P^2 - 1)$ est divisible par 3.

Montrons que *A* est divisible par 8 :

Par hypothèse, en tant que nombre premier au moins égal à 5, *P* est distinct de 2. En tant que nombre premier distinct de 2, c'est un nombre impair. Son prédécesseur $P-1$ et son successeur $P+1$ sont deux nombres pairs consécutifs. D'après le théorème T2, l'un des deux est un multiple de 4, l'autre un nombre pair non multiple de 4.

Or, le produit d'un nombre pair et d'un multiple de 4 est un multiple de 8. Il en est ainsi du produit des deux nombres $P-1$ et $P+1$: $(P-1) \times (P+1)$ est un multiple de 8.

$A = (P^2 - 1)$ est divisible par 8.

2. Déduisons-en que le nombre $A = (P^2 - 1)$ est divisible par 24 :

Soit *a* et *b* deux entiers non nuls. Nous savons qu'un entier est divisible à la fois par *a* et par *b* si et seulement s'il est divisible par leur PPCM.

- La question 1 a démontré que *A* est divisible à la fois par 3 et par 8.
- 3 et 8 sont des nombres premiers entre eux. En effet, en tant que nombre premier, 3 est premier avec tout nombre qu'il ne divise pas, ce qui est le cas du nombre 8.
- 3 et 8 étant premiers entre eux, leur PPCM est égal à leur produit :
  $PPCM(3, 8) = 3 \times 8 = 24.$

Conclusion : $A = (P^2 - 1)$ est divisible par 24.

Partie B

Dans cette partie, *P* est un nombre premier ≥ 7. Etant au moins égal 7, *P* vérifie *a fortiori* les hypothèses de la **partie A**. Nous pourrons lui appliquer le cas échéant les résultats qui ont été démontrés dans cette partie.

1. Montrons que le nombre $B = (P^4 - 1)$ est divisible par 3 et par 5 :

Le nombre $B = (P^4 - 1)$ est une différence de deux carrés et admet une factorisation :

$B = (P^2 - 1) \times (P^2 + 1) = A \times (P^2 + 1)$ où *A* est le nombre que nous avons étudié dans la **partie A** de l'exercice.

Autrement dit : $B = (P - 1) \times (P + 1) \times (P^2 + 1)$

Montrons que *B* est divisible par 3 :

B est divisible par *A* qui est lui-même divisible par 3, nous l 'avons démontré dans la **partie A**.

$B = (P^4 - 1)$ est divisible par 3.

Montrons que *B* est divisible par 5 :

Le nombre 5 étant un nombre premier, il divise le produit $B = (P - 1) \times (P + 1) \times (P^2 + 1)$ si et seulement s'il divise au moins un des trois facteurs. Nous devons démontrer que, toujours, au moins un des trois facteurs, $(P - 1)$ ou bien $(P + 1)$ ou bien $(P^2 + 1)$, est un multiple de 5.

Utilisons des congruences modulo 5. Par hypothèse, en tant que nombre premier au moins égal à 7, *P* est distinct de 5. En tant que nombre premier distinct de 5, il n'est pas multiple de 5. Si nous désignons par *r* le reste de la division euclidienne de *P* par 5, ce reste *r* est nécessairement non nul et peut prendre les valeurs 1, 2, 3 ou 4.

Construisons un tableau de congruences dans lequel nous indiquerons, suivant la valeur de *r*, des nombres auxquels sont congrus les différents facteurs de $B = (P - 1) \times (P + 1) \times (P^2 + 1)$:

Si $r = \cdots$	1	2	3	4
$P - 1 \equiv \cdots \ [5]$	0	1	2	3
$P + 1 \equiv \cdots \ [5]$	2	3	4	0
$r^2 =$	1	4	$9 = 1 \times 5 + 4$	$16 = 3 \times 5 + 1$
$P^2 \equiv \cdots \ [5]$	1	4	4	1
$P^2 + 1 \equiv \cdots \ [5]$	2	0	0	2
$B \equiv \cdots \ [5]$	0	0	0	0

Ce tableau montre que, quel que soit le cas de figure, *B* est toujours congru à 0 modulo 5.

$B = (P^4 - 1)$ est divisible par 5.

2. Montrons que le nombre $B = (P^4 - 1)$ est divisible par 16 :

Considérons la factorisation $B = A \times (P^2 + 1)$ vue au début de la **partie B,** où *A* est le nombre que nous avons étudié dans la **partie A** de l'exercice.

- D'après la **partie A**, le nombre *A* est un multiple de 8.
- Le nombre premier *P* étant distinct de 2, c'est un nombre impair. Son carré est aussi un nombre impair et le nombre $(P^2 + 1)$ est un nombre pair.

Le nombre *B* est le produit d'un multiple de 8 et d'un multiple de 2, c'est un multiple de 16.

$B = (P^4 - 1)$ est divisible par 16.

3. Déduisons-en que le nombre $B = (P^4 - 1)$ est divisible par 240 :

La propriété évoquée en **partie A.2** se généralise à trois nombres. Soit *a, b, c* trois entiers non nuls. Un entier est divisible à la fois par *a*, par *b* et par *c* si et seulement s'il est divisible par leur PPCM.

Les **questions 1 et 2** ont montré que *B* est divisible par chacun des trois nombres 3, 5 et 16.

L'entier *B* est donc divisible par leur PPCM. Précisons ce PPCM :

3 et 5 étant des nombres premiers, ils sont premiers entre eux et ils sont premiers avec tout nombre qu'ils ne divisent pas, ce qui est le cas de 16. Les trois nombres 3, 5 et 16 sont par conséquent des nombres premiers entre eux deux à deux[3]. Leur PPCM est donc égal à leur produit :

$$PPCM(3,5,16) = 3 \times 5 \times 16 = 240$$

Nous en déduisons :

$B = (P^4 - 1)$ est divisible par 240.

---

[3] « Premiers entre eux deux à deux » : C'est-à-dire que 3 et 5 sont premiers entre eux, 3 et 16 sont premiers entre eux, 5 et 16 sont premiers entre eux.
Le PPCM de trois entiers *a, b, c* « premiers entre eux deux à deux » est égal à leur produit. En effet :
$PPCM(a,b) = a \times b$ car *a* et *b* sont premiers entre eux. Alors :
$PPCM(a,b,c) = PPCM(PPCM(a,b),c) = PPCM(a \times b, c) = (a \times b) \times c$ car *c* étant premier avec *a* et avec *b*, il est premier avec leur produit.

Ne pas confondre avec trois nombres « premiers dans leur ensemble », propriété qui signifie que 1 est le seul entier > 0 qui les divise tous et qui est une propriété beaucoup plus faible. Par exemple, 10, 12 et 15 sont « premiers dans leur ensemble » mais non « premiers entre eux deux à deux ». Leur PPCM, 60, n'est pas égal à leur produit.