Maths Expertes
Terminale

Nombres Premiers

CORRIGÉ DE L'EXERCICE

Nombres premiers 09

Correction

Dans cet exercice, *q* est un nombre premier au moins égal à 7, *M* est le produit des nombres premiers de 5 à *q*, soit $M = 5 \times 7 \times \ldots \times q$, et *N* est le nombre : $N = 4M + 3$.

Nous aurons à utiliser le résultat suivant : « Soit *a* et *b* deux entiers relatifs premiers entre eux. Alors, pour tout entier relatif *k*, les entiers *a* et $b + ka$ sont premiers entre eux ».

1.a. Montrons que *N* est impair :

L'entier *N* est la somme d'un nombre pair et d'un nombre impair, donc c'est un nombre impair :

$$N = 4M + 3 = 2 \times (2M + 1) + 1$$

1.b. Montrons que *N* n'est pas congru à 0 modulo 3 :

De l'égalité $N = 4M + 3 = M + 3 \times (M + 1)$, nous déduisons que : $N - M = 3 \times (M + 1)$.

La différence $N - M$ étant un multiple de 3, nous en déduisons la congruence : $N \equiv M \quad [3]$.

Or, *M* est le produit des nombres premiers de 5 à *q*. Nous savons que deux nombres premiers distincts sont toujours des nombres premiers entre eux. Ainsi, le nombre premier 3 est premier avec chacun des nombres premiers de 5 à *q*. Etant premier avec chacun des facteurs 5, 7, …, *q*, le nombre 3 est premier avec leur produit $M = 5 \times 7 \times \ldots \times q$.

Par conséquent, *M* n'est pas un multiple de 3, il n'est pas congru à 0 modulo 3.

Puisque $N \equiv M \quad [3]$ et par transitivité, si *M* n'est pas congru à 0 modulo 3, *N* non plus :

N n'est pas congru à 0 modulo 3

2.a. Montrons que $P > q$:

Dans cette question, *P* est un nombre premier qui divise *N*.

Nous savons que tout entier > 1, comme l'est l'entier *N*, admet au moins un diviseur premier, donc l'existence d'un tel entier *P* est assurée.

Montrons qu'aucun nombre premier *P* tel que $2 \leq P \leq q$ ne divise *N*.

Les **questions 1.a** et **1.b** ont montré, respectivement, que ni 2 ni 3 ne divisaient *N* puisque *N* n'est ni pair ni multiple de 3.

Supposons maintenant que *P* soit un nombre premier tel que $5 \leq P \leq q$.

Dans ce cas, le nombre $M = 5 \times 7 \times \ldots \times q$ est un multiple de *P* car *P* est, d'après la définition de *M*, l'un des facteurs de ce produit. Le nombre $4M$ est donc lui aussi un multiple de *P*.

Compte tenu de la relation $N = 4M + 3$ définissant *N*, nous pouvons alors en déduire la congruence modulo *P* : $N \equiv 3\ [P]$. L'entier *N* n'est pas congru à 0 modulo *P*. En conséquence, quel que soit le nombre premier *P* tel que $5 \leq P \leq q$, ce nombre premier ne divise pas *N*.

Nous avons en fin de compte démontré qu'aucun nombre premier inférieur ou égal à *q* ne divise *N*.

Si *P* est un nombre premier qui divise *N*, nécessairement $P > q$.

2.b. Montrons que *P* est congru à 1 ou à 3 modulo 4 :

Nous savons que, à l'exception de 2, tous les autres nombres premiers sont des nombres impairs. Le nombre premier *P* étant au moins égal à 7, il est distinct de 2, c'est un nombre impair.

Il existe donc un entier *u* tel que : $P = 2u + 1$. Discutons suivant la parité de *u* :

- Si *u* est pair, il existe un entier *v* tel que $u = 2v$. Alors $P = 4v + 1$ et dans ce cas $P \equiv 1\ [4]$.
- Si *u* est impair, il existe un entier *v* tel que $u = 2v + 1$. Alors $P = 2(2v + 1) + 1 = 4v + 3$ et dans ce cas $P \equiv 3\ [4]$.

Ou bien $P \equiv 1\ [4]$, ou bien $P \equiv 3\ [4]$.

3.a. Montrons qu'il existe un nombre premier P_i figurant dans la décomposition de *N* qui est congru à 3 modulo 4 :

Soit $N = {P_1}^{\alpha_1} \times {P_2}^{\alpha_2} \times \ldots \times {P_r}^{\alpha_r}$ la décomposition en produit de facteurs premiers de l'entier *N*.

Nous voulons démontrer que : « Au moins un des P_i (où $i = 1, 2, \ldots, r$) est congru à 3 modulo 4 ».

Emettons l'hypothèse que la propriété contraire est vraie, c'est-à-dire supposons que : « Aucun des P_i (où $i = 1, 2, \ldots, r$) n'est congru à 3 modulo 4 ».

D'après la conclusion de la **question 2.b**, puisqu'aucun des P_i n'est congru à 3 modulo 4, c'est qu'ils sont tous congrus à 1 modulo 4.

La compatibilité de la relation de congruence modulo 4 avec la multiplication, nous permet d'en tirer deux conséquences :

- S'ils sont tous congrus à 1 modulo 4, toutes leurs puissances entières naturelles le sont aussi. En particulier, pour tout *i* tel que $1 \leq i \leq r$: ${P_i}^{\alpha_i} \equiv 1 \ [4]$
- L'entier *N* est un produit de facteurs qui sont tous congrus à 1 modulo 4. Il est donc lui-même congru à 1 modulo 4.

Sous l'hypothèse que nous avons émise, nous obtenons la congruence $N \equiv 1 \ [4]$

Or, l'entier *N* a été défini par l'égalité : $N = 4M + 3$. Il vérifie donc la congruence $N \equiv 3 \ [4]$.

Si l'hypothèse que nous avons émise était exacte, il existerait un entier congru à la fois à 1 et à 3 modulo 4. C'est impossible.

L'hypothèse « il est vrai qu'aucun des P_i (où $i = 1, 2, \ldots, r$) n'est congru à 3 modulo 4 » aboutit à une contradiction, elle doit être rejetée. Nous devons tenir pour vrai que :

« Au moins un des P_i (où $i = 1, 2, \ldots, r$) est congru à 3 modulo 4 ».

3.b. Montrons qu'il existe une infinité de nombres premiers de la forme $4n + 3$:

NB. C'est-à-dire montrons qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Nous noterons *E* l'ensemble des nombres premiers congrus à 3 modulo 4. Cet ensemble est non vide car il contient par exemple les nombres premiers 7, 11, 19, 23. Nous devons montrer que cet ensemble contient une infinité d'éléments. Nous allons pour cela « raisonner par l'absurde » une fois encore.

Emettons l'hypothèse que *E* est un ensemble fini.
En tant qu'ensemble fini non vide, *E* admet un plus grand élément. C'est-à-dire qu'il existe un nombre premier *Q* congru à 3 modulo 4 plus grand que tous les autres.

NB. Nous pouvons affirmer que nombre *Q* est au moins égal à 23, le plus grand des nombres que nous avons cités comme exemples d'éléments de *E*.

Effectuons avec cet entier *Q* la construction décrite dans l'énoncé.
Posons : $M = 5 \times 7 \times \ldots \times Q$, et considérons le nombre $N = 4M + 3$.
La **question 2** de l'exercice a montré que tous les facteurs premiers de *N* sont strictement plus grands que *Q*, et la **question 3** a montré qu'au moins l'un d'entre eux est congru à 3 modulo 4.

Si l'hypothèse que nous avons émise était exacte, il existerait un nombre premier *P* vérifiant : $\begin{cases} P > Q \\ P \in E \end{cases}$
c'est-à-dire qu'il existerait un élément de *E* strictement plus grand que le plus grand de tous. C'est impossible.

L'hypothèse « il est vrai que *E* est un ensemble fini » aboutit à une contradiction, elle doit être rejetée.
Nous devons tenir pour vrai que :

Il existe une infinité de nombres premiers congrus à 3 modulo 4, c'est-à-dire de la forme $4n + 3$.