Maths Expertes
Terminale

Arithmétique

CORRIGÉ DE L'EXERCICE

Arithmétique, Synthèse 27

Correction

Partie A. Il y a une infinité de nombres premiers

1. Montrons que le nombre $E = p_1 \times p_2 \times \ldots \times p_n + 1$ est supérieur ou égal à 2 :

Il existe au moins un nombre premier (on peut citer le nombre premier 2). L'entier *n* est au moins égal à 1 et le produit des *n* nombres premiers répertoriés $p_1 \times p_2 \times \ldots \times p_n$ est strictement positif.
En conséquence : $\boldsymbol{E \geq 2.}$

Montrons que le nombre $E = p_1 \times p_2 \times \ldots \times p_n + 1$ est premier avec chacun des p_i :

Le théorème de Bézout s'énonce ainsi : « Deux entiers relatifs *x* et *y* sont premiers entre eux si et seulement s'il existe des entiers relatifs *u* et *v* vérifiant la relation $u\,x + v\,y = 1$ ».
Nous allons utiliser sa réciproque pour montrer que, pour chaque indice *i* tel que $1 \leq i \leq n$, *E* et p_i sont premiers entre eux.

Soit *i* un indice tel que $1 \leq i \leq n$ et p_i le nombre premier d'indice *i*.

Le produit $p_1 \times p_2 \times \ldots \times p_n$ est un multiple de chacun de ses facteurs, en particulier de p_i, et de ce fait le quotient $\frac{p_1 \times p_2 \times \ldots \times p_n}{p_i}$ est un nombre entier.

Nous pouvons déduire de l'expression de *E* la relation : $E - \frac{p_1 \times p_2 \times \ldots \times p_n}{p_i} \times p_i = 1$

En posant $u = 1$ et $v = -\frac{p_1 \times p_2 \times \ldots \times p_n}{p_i}$ nous obtenons bien la relation standard de Bézout souhaitée : $u \times E + v \times p_i = 1$. Il existe deux entiers *u* et *v* qui satisfont à l'égard de *E* et de p_i la relation de Bézout.

D'après la réciproque du théorème de Bézout, pour chaque indice *i* tel que $1 \leq i \leq n$, les entiers *E* et p_i sont premiers entre eux.

2. Concluons en raisonnant par l'absurde :

NB. L'ensemble fini des diviseurs positifs autres que 1 d'un entier *E* strictement supérieur à 1 est non vide (cet ensemble contient au moins *E* lui-même). Cet ensemble admet un plus petit élément *p*.
Ce plus petit élément est nécessairement un nombre premier, sinon il aurait un diviseur strict autre que 1, qui serait lui aussi diviseur de *E* et plus petit que lui.
D'où le fait que *E* admet au moins un diviseur premier comme nous le rappelle l'énoncé.

Emettons l'hypothèse qu'il n'existe qu'un nombre fini n de nombres premiers, que nous désignons par $p_1, p_2, \ldots, p_n$.
Considérons le nombre $E = p_1 \times p_2 \times \ldots \times p_n + 1$ étudié dans la question précédente, qui est au moins égal à 2. D'après la propriété rappelée dans l'énoncé, il a au moins un diviseur premier p.
Mais E est premier avec chacun des nombres $p_1, p_2, \ldots, p_n$. Aucun de ces nombres ne divise E. En conséquence, p serait un nombre premier non répertorié parmi l'ensemble des nombres premiers : nous aboutissons à une contradiction.
Notre hypothèse « il n'existe qu'un nombre fini de nombres premiers » est à rejeter.

L'ensemble des nombres premiers est un ensemble infini.

Partie B. Etude de l'équation diophantienne associée

1.a. Reproduisons et complétons le tableau demandé :

k	2	3	4	5	6	7	8	9	10
M_k	3	7	15	31	63	127	255	511	1023

1.b. Conjecturons :

Nous constatons que les nombres M_2, M_3, M_5 et M_7, c'est-à-dire les nombres 3, 7, 31 et 127 sont tous des nombres premiers. Dans ce tableau, lorsque k est un nombre premier, le nombre M_k est lui aussi un nombre premier.

Nous pouvons légitimement conjecturer : « Si k est premier, alors M_k est premier ».

2.a. Justifions l'égalité suggérée par l'énoncé :

Nous rappelons l'identité suivante, utilisée notamment pour exprimer la somme des termes d'une suite géométrique :

Pour tout $n \in \mathbb{N}$ et pour tout réel x distinct de 1, $1 + x + x^2 + \cdots + x^n = \frac{x^{n+1}-1}{x-1}$

Soit maintenant p et q deux entiers naturels non nuls.
Le nombre $n = q - 1$ est un entier naturel et le nombre $x = 2^p$ est un réel distinct de 1.

Nous pouvons appliquer l'identité que nous venons de rappeler en utilisant ces valeurs. Elle s'écrit conformément aux attentes de l'énoncé :

$$1 + 2^p + (2^p)^2 + \cdots + (2^p)^{q-1} = \frac{(2^p)^q - 1}{2^p - 1} = \frac{2^{pq} - 1}{2^p - 1}$$

2.b. Montrons que $2^{pq} - 1$ est divisible par $2^p - 1$:

De l'égalité **2.a**, nous pouvons déduire : $2^{pq} - 1 = (2^p - 1) \times (1 + 2^p + (2^p)^2 + \cdots + (2^p)^{q-1})$

Or, le nombre $K = 1 + 2^p + (2^p)^2 + \cdots + (2^p)^{q-1}$, en tant que somme de puissances positives de 2, est un nombre entier strictement positif.

Il existe un nombre entier K tel que $2^{pq} - 1 = K \times (2^p - 1)$.

Pour tout couple (p, q) d'entiers naturels non nuls, le nombre $2^{pq} - 1$ est divisible par $2^p - 1$.

2.c. Montrons que si k n'est pas premier, M_k ne l'est pas non plus :

Soit k un entier strictement positif non premier. Il admet au moins un diviseur positif strict p (un diviseur positif autre que 1 et lui-même).

Posons $q = \frac{k}{p}$. Il s'agit par construction d'un entier strictement supérieur à 1 et nous avons l'égalité $k = pq$.

Avec les notations de la question précédente : $M_k = 2^{pq} - 1 = K \times (2^p - 1)$

Or, p et q sont ici des entiers tous deux strictement supérieurs à 1. Le nombre $2^p - 1$ est au moins égal à $2^2 - 1 = 3$ et le nombre $K = 1 + 2^p + (2^p)^2 + \cdots + (2^p)^{q-1}$ est égal à 1 augmenté d'au moins une puissance de 2, il est donc lui aussi strictement supérieur à 1. Nous avons trouvé deux diviseurs de M_k (éventuellement confondus …) qui sont, strictement, entre 1 et M_k.

Lorsque k n'est pas un nombre premier, le nombre M_k admet au moins un diviseur strict. Le nombre M_k n'est pas non plus un nombre premier.

3.a. Prouvons que M_{11} n'est pas premier :

Exprimons cet entier et décomposons-le en produit de facteurs premiers. (Pour cela, nous pouvons très bien utiliser la fonction « factor » d'une calculatrice). Nous obtenons :

$$M_{11} = 2048 - 1 = 2047 = 23 \times 89$$

Le nombre M_{11} admet deux diviseurs stricts, il n'est pas premier.

3.b. Concluons à propos de la conjecture émise en 1.b :

Nous venons de trouver un contre-exemple réfutant cette conjecture : le cas du nombre de Mersenne d'indice 11 montre qu'il existe au moins un entier k premier tel que M_k n'est pas premier.

Le théorème conjecturé « : « Si k est premier, alors M_k est premier » est faux.

NB. Nous pouvions en fait, à partir du tableau **1.a**, émettre deux conjectures :

- C1. Si k n'est pas premier, M_k n'est pas premier.
- C2. Si k est premier, M_k est premier.

La **question 2** a pour objectif de démontrer la proposition C1. Nous y démontrons en effet, universellement, que quel que soit l'entier k non premier, la nombre M_k n'est pas premier.

La **question 3** a pour objectif de réfuter la conjecture C2. Nous y démontrons qu'il existe un nombre k premier, en l'occurrence le nombre 11, tel que M_k n'est pas premier.

Le cas du nombre 11, pour lequel la proposition C2 est fausse, est un « contre-exemple ».

Pour prouver qu'une proposition est fausse, une méthode consiste à proposer un contre-exemple qui réfute cette proposition. Un seul contre-exemple suffit.