Maths Expertes
Terminale

Nombres Premiers

CORRIGÉ DE L'EXERCICE

Nombres premiers

07

Correction

Soit n un entier ≥ 1 et f_n la fonction polynôme définie pour tout réel x par : $f_n(x) = x^n - 1$.

Rappelons une factorisation remarquable de cette fonction polynôme :

Pour tout réel x, $\quad f_n(x) = x^n - 1 = (x-1) \times (1 + x + x^2 + \cdots + x^{n-1})$

Nous utiliserons aussi dans cet exercice une caractérisation d'un nombre entier $n > 1$ non premier :

- Un entier $n > 1$ est non premier si et seulement s'il[1] est le produit $n = p \times q$ de deux entiers p et q tous deux au moins égaux à 2.

1.a. Vérifions que $2^{pq} - 1 = (2^p - 1) \times \left(1 + 2^p + 2^{2p} + \cdots + 2^{(q-1)p}\right)$:

NB. p et q sont des entiers naturels supérieurs ou égaux à 2.

Soit la fonction polynôme f_q définie sur $\mathbb{R}$ conformément à notre préambule : $f_q(x) = x^q - 1$.

Utilisons sa factorisation remarquable.

Pour tout $x \in \mathbb{R}$, $\quad f_q(x) = x^q - 1 = (x-1) \times (1 + x + x^2 + \cdots + x^{q-1})$.

Ecrivons cette factorisation avec la valeur numérique $x = 2^p$:

$f_q(2^p) = (2^p)^q - 1 = (2^p - 1) \times (1 + 2^p + (2^p)^2 + \cdots + (2^p)^{q-1})$.

En vertu des règles de calcul sur les puissances, on sait que pour tout entier $k > 0$: $(2^p)^k = 2^{kp}$.

Nous obtenons l'identité souhaitée :

$$f_q(2^p) = 2^{pq} - 1 = (2^p - 1) \times \left(1 + 2^p + 2^{2p} + \cdots + 2^{(q-1)p}\right).$$

---

[1] En effet, si $n = p \times q$ avec p et q tous deux au moins égaux à 2, alors $n \geq 2p > p$. Le nombre p vérifie la double inégalité $1 < p < n$, c'est un diviseur strict de n, l'entier n n'est pas premier. Réciproquement, si $n > 1$ n'est pas premier, il admet un diviseur strict p (tel que $1 < p < n$). Soit q le quotient de la division de n par p. Cet entier q vérifie la relation $n = p \times q$ et l'inégalité $p < n$ implique l'inégalité $q > 1$. Les deux entiers p et q dont n est le produit sont tous deux au moins égaux à 2.

1.b. Déduisons-en que, si *n* n'est pas premier, M_n ne l'est pas non plus :

Soit *n* un entier tel que $n \geq 1$. Si *n* n'est pas premier, alors :

- Ou bien il est égal à 1. Le nombre de Mersenne qui lui est associé est $M_1 = 2^1 - 1 = 1$. Ce nombre de Mersenne M_1 n'est pas premier non plus.
- Ou bien $n > 1$ et, d'après le préambule, il est le produit de deux entiers *p* et *q* tous deux au moins égaux à 2. Nous pouvons appliquer le résultat de la **question 1.a** :

$$M_n = 2^n - 1 = 2^{pq} - 1 = (2^p - 1) \times \left(1 + 2^p + 2^{2p} + \cdots + 2^{(q-1)p}\right)$$

  Puisque $p \geq 2$, $2^p - 1 \geq 2^2 - 1 = 3$, et puisque $q \geq 2$, le deuxième facteur contient au moins deux termes : $1 + 2^p + 2^{2p} + \cdots + 2^{(q-1)p} \geq 1 + 2^p \geq 1 + 2^2 \geq 5$. Les entiers $(2^p - 1)$ et $\left(1 + 2^p + 2^{2p} + \cdots + 2^{(q-1)p}\right)$ ont pour produit M_n et sont tous deux plus grands que 2, le nombre M_n n'est pas premier.

Quel que soit l'entier $n \geq 1$, si *n* n'est pas premier, M_n ne l'est pas non plus.

1.c. Déterminons, pour $n \leq 12$, ceux des nombres M_n qui sont premiers :

D'après la question précédente, ceux des nombres M_n d'indice ≤ 12 qui sont susceptibles d'être premiers sont les nombres $M_2, M_3, M_5, M_7, M_{11}$ (ceux dont l'indice est un nombre premier).

Nous avons défini sur une calculatrice TI-Nspire-CAS la fonction $m(n) = 2^n - 1$ donnant le nombre de Mersenne de rang *n*. Nous avons ensuite calculé les nombres de Mersenne de rangs 2, 3, 5, 7 et 11 et testé leur primalité.	Define $m(n)=2^n-1$	*Terminé*
	$\{m(2),\text{isPrime}(m(2))\}$	$\{3,\text{true}\}$
	$\{m(3),\text{isPrime}(m(3))\}$	$\{7,\text{true}\}$
	$\{m(5),\text{isPrime}(m(5))\}$	$\{31,\text{true}\}$
	$\{m(7),\text{isPrime}(m(7))\}$	$\{127,\text{true}\}$
	$\{m(11),\text{isPrime}(m(11))\}$	$\{2047,\text{false}\}$
	factor(2047)	$23 \cdot 89$

La copie d'écran que nous avons reproduite montre que :

M_2, M_3, M_5, M_7 sont premiers et ce sont les seuls parmi ceux d'indice ≤ 12

2.a. Justifions que si M_n est premier, alors n est premier :

Nous devons justifier l'implication :

« M_n est premier implique que n est premier ».

L'implication contraposée[2] de cette implication est l'implication :

« n est non premier implique que M_n est non premier ».

C'est exactement l'implication que nous avons démontrée dans la **question 1.b**.

Or, nous savons que démontrer l'une des deux implications, la directe ou la contraposée, revient à démontrer l'autre.

Ainsi, la démonstration faite dans la **question 1.b** démontre aussi en même temps, par contraposition, son implication contraposée. Nous pouvons affirmer :

Si M_n est un nombre premier, alors n est un nombre premier.

2.b. Examinons si la réciproque est vraie ou fausse :

L'implication réciproque s'énonce ainsi : « n est premier implique que M_n est premier ».

Or, la **question 1.c** nous a montré que le nombre de Mersenne $M_{11} = 2047 = 23 \times 89$ est un nombre composé (réponse « false » au test de primalité) alors que son indice 11 est un nombre premier.

Nous disposons d'un contre-exemple qui infirme l'implication réciproque et nous savons qu'un seul contre-exemple suffit à démontrer qu'une propriété est fausse.

L'implication réciproque est fausse.

NB. Le contre-exemple $n = 11$ n'est pas isolé. L'algorithme ci-contre montre que M_{23}, M_{29} et M_{37} ne sont pas non plus des nombres premiers.	*mersenne*(40)
	$\{11,2047,23\cdot 89\}$
	$\{23,8388607,47\cdot 178481\}$
	$\{29,536870911,233\cdot 1103\cdot 2089\}$
	$\{37,137438953471,223\cdot 616318177\}$
	Terminé
		mersenne 3/5
		Define **mersenne**(a)=
		Prgm
		For i,1,a
		If isPrime (i)=true and isPrime $(m(i))$=false Then
		Disp $\{i,m(i),\text{factor}(m(i))\}$
		EndIf
		EndFor
		EndPrgm

---

[2] Etant donné une implication « $A \Rightarrow B$ », l'implication contraposée est : « $nonB \Rightarrow nonA$ ».

Démontrer l'une des deux implications, directe ou contraposée, revient à démontrer l'autre.

En effet, si « $A \Rightarrow B$ » est vraie, on ne peut pas avoir à la fois $nonB$ et *A* (car on aurait en même temps *B* et *nonB*) et si « $nonB \Rightarrow nonA$ » est vraie, on ne peut pas avoir à la fois *A* et non *B* (car on aurait en même temps *A* et *nonA*).