Pour tout entier naturel non nul n, on pose $M_n = 2^n - 1$. M_n est appelé nombre de Mersenne.

Partie A. Exploration. Premiers résultats

1. Pour $1 \leq p \leq 20$, déterminer si M_p est premier ou composé. Qu'observe-t-on quand p est composé ? quand p est premier ?
2. Vérifier que, pour tout entier n : $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + ... + a + 1)$
   En déduire que (p composé) $\Rightarrow$ (M_p composé)
3. On suppose désormais que M_p admet un diviseur premier d. Justifier les résultats :
   a. $2^p \equiv 1\ (d)$;
   b. $2^{d-1} \equiv 1\ (d)$.

Si p est composé, tous les M_p sont composés.
D'après la question A 1, si p est premier, il existe des M_p composés, ce sont leurs diviseurs qu'on va étudier de plus près.

Partie B. Etude du cas où p est premier

On considère un entier p premier tel que $M_p = 2^p - 1$ admette un diviseur premier d.
Soit I l'ensemble des nombres premiers n tels que $2^n \equiv 1\ (d)$

1. Justifier que I n'est pas vide et qu'il admet un plus petit élément p_0 strictement supérieur à 1.
2. En écrivant la division euclidienne de n par p_0, démontrer que tout élément de I est un multiple de p_0.
   En déduire que $p_0 = p$.
3. On admet que $2^{d-1} \equiv 1(d)$.
   Déduire que p_0 divise $d - 1$ puis qu'il existe k dans $\mathbb{N}$ tel que $d = 2kp + 1$.

Partie C. Etude de deux nombres de Mersenne

1. L'entier $M_{19} = 2^{19} - 1 = 524\,287$
   D'après la question B.3, les diviseurs premiers de M_{19} sont de la forme $d = 38k + 1$ avec $k \in \mathbb{N}$.

a. Combien y-a-t-il de diviseurs de la forme $d = 38k + 1$ avec $d < E(\sqrt{M_{19}})$?

b. Démontrer que si k prend l'une des formes $3m + 1$, $5m + 3$, $7m + 2$ avec $m \in \mathbb{N}$, d n'est pas premier.

c. Combien y a-t-il finalement de cas à examiner ? M_{19} est-il premier ?

2. L'entier $M_{23} = 2^{23} - 1 = 8\,388\,607$
   Quel est le premier diviseur possible de M_{23} d'après la question B.3 ?
   M_{23} est-il premier ?

CORRECTION

Partie A. Exploration. Premiers résultats

1. p est un nombre entier non nul donc les cas possibles sont :

p	1	2	3	4	5	6	7	8	9	10
M_p	1	3	7	15	31	63	127	255	511	1023
M_p	non premier	premier	premier	3×5	premier	7×9	premier	5×51	7×73	3×341

p	11	12	13	14	15	16	17	18	19
M_p	2047	4095	8191	16383	32767	65535	131071	262143	524287
M_p	23×89	5×819	premier	3×5461	7×4681	5×13107	premier	3×87381	premier

Pour $0 \leq p \leq 19$, si p est composé, M_p est composé.
La réciproque est fausse, M_{11} est composé et 11 n'est pas composé.
Lorsque p est premier ($p \in \{2 ; 3 ; 5 ; 7 ; 13 ; 17 ; 19\}$, certains M_p sont premiers.

2. si a est un réel différent de 1 alors $a^{n-1} + a^{n-2} + ... + a + 1 = \dfrac{a^n - 1}{a - 1}$ donc $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + ... + a + 1)$

si $a = 1$, $a^n = 1$ donc $a^n - 1 = 0$ et $(a - 1) = 0$ donc $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + ... + a + 1) = 0$
La relation est vérifiée pour tout entier n et tout réel a.

Si p est composé alors il existe q et q' deux entiers naturels q et q' compris ente 2 et $p - 1$ tels que $p = q\,q'$.
$a^p = (a^{q'})^q$ donc en posant $b = a^{q'}$, on a : $a^p - 1 = b^q - 1$
$b^q - 1 = (b - 1)(b^{q-1} + b^{q-2} + ... + b + 1)$
donc $a^p - 1 = (a^{q'} - 1)(a^{q'(q-1)} + a^{q'(q-2)} + ... + a^{q'} + 1)$
pour $a = 2$: $2^p - 1 = (2^{q'} - 1)(2^{q'(q-1)} + 2^{q'(q-2)} + ... + 2^{q'} + 1)$
$2 \leq q' \leq p - 1$ donc $2^2 \leq 2^{q'} \leq 2^{p-1} < 2^p$ soit $3 \leq 2^{q'} - 1 \leq 2^{p-1} - 1 < 2^p - 1$
$2^{q'} - 1$ est différent de 1 et M_p et est un diviseur de M_p donc M_p n'est pas un nombre premier.
Si p est composé alors M_p est composé.

3. *a*. d divise M_p donc $M_p \equiv 0\ (d)$ soit $2^p \equiv 1\ (p)$
M_p est un nombre impair donc 2 ne divise pas M_p.
d est un nombre premier différent de 2 donc 2 et d sont premiers entre eux.

D'après le petit théorème de Fermat :
d est un nombre premier et 2 est un entier non divisible par d, alors $2^{d-1} - 1$ est un multiple de p donc $2^{d-1} \equiv 1\ (d)$

Partie B. Etude du cas où *p* est premier

1. $2^{d-1} \equiv 1\ (d)$ donc $d - 1 \in$ I, donc I n'est pas vide.
Les éléments de I sont des nombres premiers donc sont supérieurs ou égaux à 2 donc I admet un plus petit élément p_0 strictement supérieur à 1.

2. En effectuant la division euclidienne de n par p_0, il existe deux entiers q et r tels que $n = p_0 q + r$ avec $0 \leq r \leq p_0 - 1$.
$2^n = (2^{p_0})^q \times 2^r$ or $2^{p_0} \equiv 1\,(p)$ donc $(2^{p_0})^q \times 2^r \equiv 2^r\ (d)$
or $2^n \equiv 1\ (d)$ donc $2^r \equiv 1\,(d)$ donc $r \in$ I
p_0 est le plus petit élément de I et est strictement supérieur à 1, or $0 < r < p_0$ donc $r = 0$ (sinon r serait le plus petit élément de I et non p_0) donc tout élément n de I est un multiple de p_0.
$p \in$ I donc p est un multiple de p_0, or p est un nombre premier donc $p_0 = p$.

3. $2^{d-1} \equiv 1\ (d)$ donc $d - 1 \in$ I
d'après la question précédente, $d - 1$ est un multiple de p_0
donc p_0 divise $d - 1$.
$p_0 = p$ donc il existe q dans $\mathbb{N}$ tel que $d - 1 = q\,p$.
si $p = 2$, M_2 est un nombre premier donc p est un nombre premier impair, ses diviseurs sont donc impairs donc d est un nombre premier impair
donc $d - 1$ est pair, donc 2 divise $d - 1$ donc 2 divise $q\,p$
p est impair donc 2 et p sont premiers entre eux donc d'après le théorème de Gauss, 2 divise q donc il existe k dans $\mathbb{N}$ tel que $q = 2k$ donc $d - 1 = 2\,k\,p$ donc il existe k dans $\mathbb{N}$ tel que $d = 2\,k\,p + 1$

Partie C. Etude de deux nombres de Mersenne

1. L'entier $M_{19} = 2^{19} - 1 = 524287$
D'après la question B.3, les diviseurs premiers de M_{19} sont de la forme $d = 38\,k + 1$ avec $k \in \mathbb{N}$.

a. d est un nombre premier impair donc $d \geq 3$
$d \leq E(\sqrt{M_{19}})$ or $E(\sqrt{M_{19}}) = 724$ donc $3 \leq d \leq 724$
$3 \leq 38\,k + 1 \leq 724$ donc $\frac{1}{19} \leq k \leq \frac{362}{19}$, k est un nombre entier donc $1 \leq k \leq 19$, il existe donc 18 possibilités pour d,

b. si k prend la forme $3\,m + 1$, alors $38\,k + 1 = 3 \times 38\,m + 39$ donc 3 divise $38\,k + 1$ donc d n'est pas premier.
si k prend la forme $5\,m + 3$, alors $38\,k + 1 = 5 \times 38\,m + 115$ donc 5 divise $38\,k + 1$ donc d n'est pas premier.
si k prend la forme $7\,m + 2$, alors $38\,k + 1 = 7 \times 38\,m + 77$ donc 7 divise $38\,k + 1$ donc d n'est pas premier.

c.

k	~~1~~	~~2~~	~~3~~	~~4~~	5	6	~~7~~	~~8~~	~~9~~	~~10~~	~~11~~	~~12~~	~~13~~	~~14~~	~~15~~	~~16~~	~~17~~	~~18~~	~~19~~
$38\,k + 1$	~~39~~	~~77~~	~~115~~	~~153~~	191	229	~~267~~	~~305~~	~~343~~	~~381~~	~~419~~	~~457~~	~~495~~	~~533~~	~~571~~	~~609~~	~~647~~	~~685~~	~~723~~

d est un nombre premier donc les possibilités sont 191 ; 229 ; 419 ; 457 ; 571 ; 647, aucun de ces nombres divise M_{19} donc M_{19} est premier.

2. L'entier $M_{23} = 2^{23} - 1 = 8\,388\,607$
D'après la question B.3, les diviseurs premiers de M_{23} sont de la forme $d = 46\,k + 1$ avec $k \in \mathbb{N}$, le premier diviseur possible de M_{23} est donc 47.
$8\,388\,607 = 47 \times 178\,481$ donc M_{23} n'est pas premier.