On appelle nombres de MERSENNE les nombres de la forme $M_p = 2^p - 1$, avec p entier premier impair.
Soit q un facteur premier de M_p.

1. Quelle est la parité de q ?
2. Démontrer que p est le plus petit entier supérieur à 1 vérifiant $2^p \equiv 1\ (q)$.
3. Démontrer que p divise $q - 1$.
4. On écrit alors $q - 1 = p \times m$, avec $m \in \mathbb{N}$. Démontrer que m est pair et en déduire que : $q \equiv 1\ (2p)$
5. **Application :** les nombres M_{17} ; M_{19} ; et M_{23} sont-ils premiers ?

CORRECTION

1. $p \geq 2$ donc 2^p est un nombre pair supérieur ou égal à 8 donc $2^p - 1$ est impair donc q est impair.

2. q est un facteur premier de M_p, donc il existe un entier Q tel que $M_p = q$ Q donc $M_p \equiv 0\ (q)$ donc $2^p \equiv 1\ (q)$
L'ensemble des entiers naturels tels que $2^n \equiv 1\ (q)$ n'est donc pas vide, soit p' le plus petit élément de cet ensemble.
On a donc $p \geq p$' et $2^{p'} \equiv 1\ (q)$

Effectuons la division euclidienne de p par p', il existe deux entiers k et r tels que $p = p'\ k + r$ avec $0 \leq r < p$'
si $0 < r < p$' alors $2^p = 2^{p'\ k + r} = (2^{p'})^k \times 2^r$, comme $2^p \equiv 1\ (q)$ et $2^{p'} \equiv 1\ (q)$ alors $2^r \equiv 1\ (q)$ or $r < p$' ce qui est en contradiction avec l'hypothèse p' le plus petit élément de cet ensemble. donc on ne peut pas avoir $0 < r < p$' donc $r = 0$
si $r = 0$ alors p' divise p or p est un nombre premier donc $p' = p$ ou $p' = 1$
donc p est le plus petit entier strictement supérieur à 1 vérifiant $2^p \equiv 1\ (q)$.

3. Effectuons la division euclidienne de $q - 1$ par p, il existe deux entiers k et r tels que $q - 1 = p\ k + r$ avec $0 \leq r < p$
$2^{q-1} = (2^p)^k \times 2^{r\ r}$, comme $2^p \equiv 1\ (q)$ alors $2^{q-1} \equiv 2^r\ (q)$
q est un nombre premier, donc $2^{q-1} \equiv 1\ (q)$ (petit théorème de Fermat)
donc $2^r \equiv 1\ (q)$ or p est le plus petit entier strictement supérieur à 1 vérifiant $2^p \equiv 1\ (q)$ donc $r = 0$ donc p divise $q - 1$.

4. q est un nombre premier diviseur de M_p or M_p est un nombre impair donc q est impair et $q - 1$ est pair
2 divise $p \times m$ or p est un entier premier impair donc 2 est premier avec p donc 2 divise m (théorème de Gauss) donc m est pair.
Il existe un entier m' tel que $m = 2$ m' donc $q - 1 = p \times 2$ m' $= (2p)$ m' donc $q - 1 \equiv 0\ (2p)$ donc $q \equiv 1\ (2p)$

5. **Application :** 17 est un nombre premier, d'après les questions précédentes :si q est un diviseur premier de M_{17}, alors $q \equiv 1\ (2 \times 17)$ donc $q - 1 = 34\ k$ soit $q = 34\ k + 1$
$M_{17} = 2^{17} - 1 = 131\ 071$ donc $362 < \sqrt{M_{17}} < 363$
donc il faut chercher des nombres premiers inférieurs à 362, de la forme $34\ k + 1$ qui diviserait M_{17}

k	0	1	2	3	4	5	6	7	8	9	10
q	~~1~~	~~35 $= 5 \times 7$~~	~~69 $= 3 \times 13$~~	103	137	~~171 $= 3 \times 57$~~	~~205 $= 5 \times 41$~~	239	~~273 $= 3 \times 91$~~	307	~~341 $= 11 \times 31$~~

103 ; 137 ; 239 et 307 ne divisent pas 131 071 donc M_{17} est un nombre premier.

19 est un nombre premier, d'après les questions précédentes, si q est un diviseur premier de M_{19}, alors $q \equiv 1\ (2 \times 19)$
donc $q - 1 = 38\ k$ soit $q = 38\ k + 1$;
$M_{19} = 2^{19} - 1 = 524\ 287$ donc $724 < \sqrt{M_{19}} < 725$ donc il faut chercher des nombres premiers inférieurs à 724, de la forme $38\ k + 1$ qui diviserait M_{19}

k	q		k	q
0	1		10	381 $= 3 \times 127$
1	$39 = 3 \times 13$		11	419
2	$77 = 7 \times 11$		12	457
3	$115 = 5 \times 23$		13	495 $= 5 \times 99$
4	$153 = 17 \times 9$		14	533 $= 13 \times 41$
5	191		15	571
6	229		16	609 $= 3 \times 203$
7	$267 = 3 \times 89$		17	647
8	$305 = 5 \times 61$		18	685 $= 5 \times 137$
9	$343 = 7 \times 49$		19	723 $= 3 \times 241$

Aucun des nombres premiers 191 ; 229 ; 419 ; 571 ; 647 ne divise M_{19} donc M_{19} est un nombre premier.

23 est un nombre premier, d'après les questions précédentes, si q est un diviseur premier de M_{19}, alors $q \equiv 1\ (2 \times 23)$
donc $q - 1 = 46\ k$ soit $q = 46\ k + 1$; $M_{23} = 2^{19} - 1 = 8\ 388\ 607$ donc $2897 < \sqrt{M_{23}} < 2897$
donc il faut chercher des nombres premiers inférieurs à 2897, de la forme $46\ k + 1$ qui diviserait M_{23}
si k = 1 alors q = 47 or $M_{23} = 47 \times 178\ 481$ donc M_{23} n'est pas un nombre premier