## Thème : Des nombres particuliers : Mersenne, Fermat, Carmichael

### Corrigé de l'activité 1. Nombres de Mersenne (5 exercices)

## Exercice 1

1) On fait la table de valeurs de $2^X - 1$ avec un début de table à $X = 1$ et un pas de 1. On obtient les valeurs :

| $n$ | Nombre de Mersenne $M_n$ | Valeur |
|---|---|---|
| 1 | $M_1 = 2^1 - 1$ | $M_1 = 1$ |
| 2 | $M_2 = 2^2 - 1$ | $M_2 = 3$ |
| 3 | $M_3 = 2^3 - 1$ | $M_3 = 7$ |
| 4 | $M_4 = 2^4 - 1$ | $M_4 = 15$ |
| 5 | $M_5 = 2^5 - 1$ | $M_5 = 31$ |
| 6 | $M_6 = 2^6 - 1$ | $M_6 = 63$ |
| 7 | $M_7 = 2^7 - 1$ | $M_7 = 127$ |
| 8 | $M_8 = 2^8 - 1$ | $M_8 = 255$ |
| 9 | $M_9 = 2^9 - 1$ | $M_9 = 511$ |
| 10 | $M_{10} = 2^{10} - 1$ | $M_{10} = 1023$ |
| 11 | $M_{11} = 2^{11} - 1$ | $M_{11} = 2047$ |
| 12 | $M_{12} = 2^{12} - 1$ | $M_{12} = 4095$ |
| 13 | $M_{13} = 2^{13} - 1$ | $M_{13} = 8191$ |
| 14 | $M_{14} = 2^{14} - 1$ | $M_{14} = 16383$ |
| 15 | $M_{15} = 2^{15} - 1$ | $M_{15} = 32767$ |
| 16 | $M_{16} = 2^{16} - 1$ | $M_{16} = 65535$ |
| 17 | $M_{17} = 2^{17} - 1$ | $M_{17} = 131071$ |
| 18 | $M_{18} = 2^{18} - 1$ | $M_{18} = 262143$ |
| 19 | $M_{19} = 2^{19} - 1$ | $M_{19} = 524287$ |
| 20 | $M_{20} = 2^{20} - 1$ | $M_{20} = 1048575$ |

2) Les nombres premiers dans le tableau ci-dessus sont surlignés.

3) a) Conjecture : Si $n$ est composé alors $M_n$ est composé.

b) Si $n$ est premier alors $M_n$ est composé ou bien $M_n$ est premier. Par exemple, pour $n = 11$ premier on a le cas où $M_{11} = 2047 = 23 \times 89$ est composé et pour $n = 7$ premier on a le cas où $M_7 = 127$ est premier.

## Exercice 2

**Partie A : Exemples**

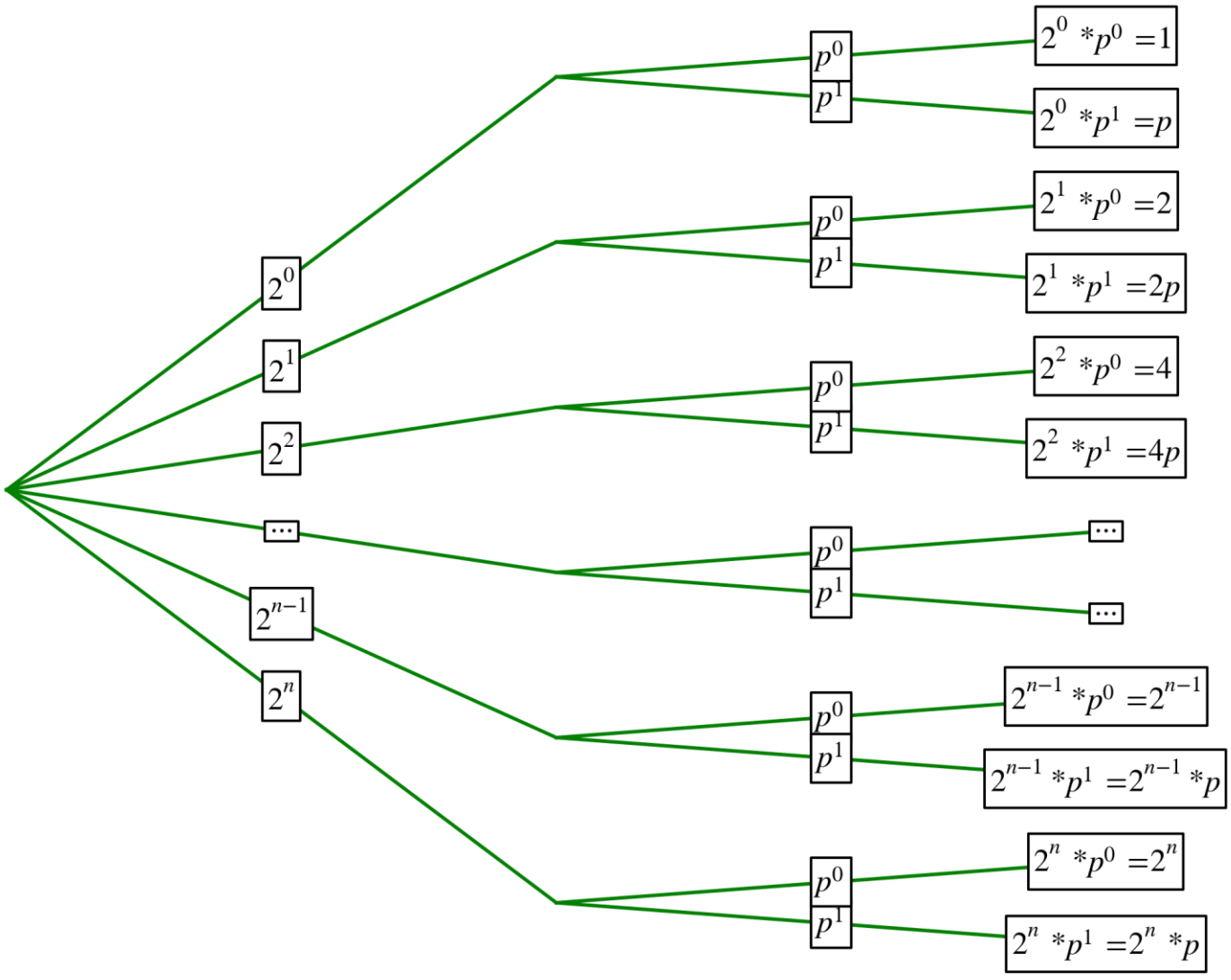
Les diviseurs propres de 6 sont $1, 2, 3$.
Leur somme $S = 1 + 2 + 3 = 6$. Donc $a = S$. Donc $a = \mathbf{6}$ est parfait.

Les diviseurs propres de 28 sont $1, 2, 4, 7, 14$.
Leur somme $S = 1 + 2 + 4 + 7 + 14 = 28$. Donc $a = S$. Donc $a = \mathbf{28}$ est parfait.

2) $6 = 2^1 \times 3$ donc $6 = 2^n \times (2^{n+1} - 1)$ avec $n = 1$ et où $p = 2^{n+1} - 1$ est premier.
$28 = 2^2 \times 7$ donc $28 = 2^n \times (2^{n+1} - 1)$ avec $n = 2$ et où $p = 2^{n+1} - 1$ est premier.

**Partie B : Cas général**

1) a) Les diviseurs de $a$ sont les entiers de la forme $2^{\alpha_1} \times p^{\alpha_2}$ avec $\alpha_1 \in \{0 ; 1 ; 2 ; \dots ; n\}$ et $\alpha_2 \in \{0 ; 1\}$.
Il y a donc $(n + 1) \times 2$ diviseurs. On peut faire un arbre pour les visualiser :




Les diviseurs propres sont donc : $1,\ p,\ 2,\ 2p,\ 4,\ 4p, \dots,\ 2^{n-1},\ 2^{n-1}p,\ 2^n$. Il y en a $(n + 1) \times 2 - 1 = 2n + 1$.

b) Leur somme est : $S = 1 + p + 2 + 2p + 4 + 4p + \cdots + 2^{n-1} + 2^{n-1}p + 2^n.$

$$S = (1+p) + 2(1+p) + 4(1+p) + \cdots + 2^{n-1}(1+p) + 2^n$$

$$S = (1+p)(1 + 2 + 4 + \cdots + 2^{n-1}) \ + 2^n$$

$$S = (1+p) \times \frac{1-2^n}{1-2} + 2^n$$

$$S = (1+p) \times \frac{2^n-1}{2-1} + 2^n$$

$$\boldsymbol{S = (1+p) \times (2^n - 1) + 2^n}$$

La somme des diviseurs propres de $a = 2^n \times p$ est donc $S = (1 + \boldsymbol{p}) \times (2^n - 1) + 2^n$

2) a) Si $p = 2^{n+1} - 1$ alors :

$$S = \left(1 + \boldsymbol{2^{n+1} - 1}\right) \times (2^n - 1) + 2^n$$

$$S = 2^{n+1} \times (2^n - 1) + 2^n$$

$$S = 2^{n+1} \times 2^n - 2^{n+1} + 2^n$$

$$S = 2^{n+1} \times 2^n - 2^n \times 2 + 2^n$$

$$S = 2^n(2^{n+1} - 2 + 1)$$

$$S = 2^n(2^{n+1} - 1)$$

b) On sait que « $a$ est parfait » équivaut à « $a$ est égal à la somme de ses diviseurs propres » c'est-à-dire $a = S$.
Or on suppose que $a = 2^n \times p$ et que $p = 2^{n+1} - 1$ où $p$ est premier.

Donc on a : $a = 2^n \times (2^{n+1} - 1)$.

Donc on a bien $a = S$.

***Conclusion :***

Si on a : $a = 2^n \times (2^{n+1} - 1)$ avec $2^{n+1} - 1$ premier, alors $a$ est parfait.

3) a) Le résultat démontré est :
Si un entier naturel $a$ peut s'écrire $a = 2^n \times (2^{n+1} - 1)$ avec $2^{n+1} - 1$ premier

ou encore

Si $a$ peut s'écrire $a = 2^n \times M_{n+1}$ où $M_{n+1} = 2^{n+1} - 1$ est un nombre de Mersenne premier, alors $a$ est parfait.

b) Pour donner deux autres nombres parfaits, il suffit de prendre deux nombres de Mersenne premiers. Par exemple en utilisant le tableau de l'exercice 1 :

| $n$ | Nombre de Mersenne $M_n$ | Valeur de $M_n$ | $a = 2^{n-1} \times M_n$ |
|---|---|---|---|
| 2 | $M_2 = 2^2 - 1$ | $M_2 = 3$ | $2^1 \times M_2 = 6$ |
| 3 | $M_3 = 2^3 - 1$ | $M_3 = 7$ | $2^2 \times M_3 = 28$ |
| 5 | $M_5 = 2^5 - 1$ | $M_5 = 31$ | $2^4 \times M_5 = \mathbf{496}$ |
| 7 | $M_7 = 2^7 - 1$ | $M_7 = 127$ | $2^6 \times M_7 = \mathbf{8128}$ |
| 13 | $M_{13} = 2^{13} - 1$ | $M_{13} = 8191$ | $2^{12} \times M_{13} = \mathbf{33550336}$ |
| 17 | $M_{17} = 2^{17} - 1$ | $M_{17} = 131071$ | $2^{16} \times M_{17} = \mathbf{8589869056}$ |
| 19 | $M_{19} = 2^{19} - 1$ | $M_{19} = 524287$ | $2^{18} \times M_{19} \approx 1{,}37.10^{11}$ |

## Exercice 3

1) a) Soit $S = 2^{p(q-1)} + 2^{p(q-2)} + \cdots + 2^p + 1$.

$S$ est une somme de termes consécutifs de la suite géométrique de premier terme $1$ et de raison $2^p$. Cette somme comporte $q$ termes. Donc :

$$S = 1 \times \frac{1 - (2^p)^q}{1 - 2^p}$$

$$S = \frac{2^{pq} - 1}{2^p - 1}$$

Ainsi :

$$2^{pq} - 1 = (2^p - 1)S$$

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

b) Un nombre de Mersenne s'écrit $M_n = 2^n - 1$ où $n$ est un entier naturel non nul.

On suppose dans cette question que $n$ est composé. Donc il existe deux entiers $p$ et $q$ strictement supérieurs à $1$ tels que $n = pq$.

Donc $M_n$ s'écrit $M_n = 2^{pq} - 1$

En utilisant le résultat de la question 1) a), on a :

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

Puisque $p \geq 2$, on a $2^p \geq 4$.

$(2^p - 1) \geq 3$ et $\left(2^{p(q-1)} + 2^{p(q-2)} + \cdots + 2^p + 1\right) \geq 5$.

Donc $M_n$ est le produit de deux facteurs strictement supérieurs à $1$. Donc si $n$ est composé alors $M_n$ est composé.

2) Puisque si $n$ est composé alors $M_n$ est composé, alors il faut chercher parmi les indices $n$ premiers pour trouver un nombre de Mersenne premier.

## Exercice 4

**Partie A : *Forme d'un diviseur d d'un nombre de Mersenne $M_p$ avec p premier***

1) Par hypothèse, le nombre de Mersenne $M_p$ où $p$ est un nombre premier, est divisible par $d$ où $d$ est un nombre lui aussi premier. Donc on a :

$$M_p \equiv 0 \quad (d).$$

D'après la définition des nombres de Mersenne, on a $M_p = 2^p - 1$. Donc :

$$2^p - 1 \equiv 0 \quad (d).$$

$$2^p \equiv 1 \quad (d).$$

2) a) D'après la question 1), on a comme hypothèse $2^p \equiv 1 \quad (d)$.
Par hypothèse, $n = p$ est une valeur qui satisfait à la définition de l'ensemble $I$.

- Donc l'ensemble $I$ contient au moins un élément qui est $p$. Donc l'ensemble $I$ n'est pas vide.
- Tout ensemble d'entiers naturels non vide contient un plus petit élément noté ici $p_0$.
- Puisque la relation $2^1 \equiv 1 \quad (d)$ est fausse quel que soit le nombre premier $d$ alors $n = 1$ n'appartient pas à l'ensemble $I$. Le plus petit élément $p_0$ de l'ensemble $I$ est donc strictement supérieur à 1.

b) $n$ est un élément quelconque de $I$. Puisque $n \in I$, par définition de $I$, on a $2^n \equiv 1 \quad (d)$.
On a noté $p_0$ le plus petit élément de $I$.

- La division euclidienne de $n$ par $p_0$ s'écrit $n = p_0 q + r$ avec $0 \leq r < p_0$ et $q \in \mathbb{N}^*$ puisque $p_0$ est le plus petit élément de $I$.

  Pour tout élément $n$ de $I$ on a donc :

$$2^{p_0 q + r} \equiv 1 \quad (d)$$

$$(2^{p_0})^q \times 2^r \equiv 1 \quad (d)$$

  $p_0$ étant un élément de $I$, on a $2^{p_0} \equiv 1 \quad (d)$. Donc :

$$(1)^q \times 2^r \equiv 1 \quad (d)$$

$$2^r \equiv 1 \quad (d)$$

- Supposons que le reste $r$ est non nul. Dans ce cas, il vérifie $2^r \equiv 1 \quad (d)$, donc $r \in I$.

  Et comme $r$ est tel que $0 \leq r < p_0$ alors $r$ est un élément de $I$, tout en étant strictement inférieur au plus petit élément de $I$. C'est absurde. On en déduit que la proposition « $r$ est non nul » est fausse.

  Conclusion : $r = 0$ et donc tout élément $n$ de $I$ vérifie $n = p_0 q$ avec $q \geq 1$

- $I$ contient donc un plus petit élément $p_0$ et ses multiples. Or d'après 2)a) le nombre premier $p$ appartient à $I$. Comme aucun des multiples de $p_0$ n'est premier, on déduit que $p$ est le plus petit élément de $I$.

  Conclusion : $p = p_0$.

c) On admet que $2^{d-1} \equiv 1 \quad (d)$. Donc $d - 1 \in I$.
Donc - soit $d - 1$ est égal à $p$ qui est le plus petit élément de $I$,

- soit $d - 1$ est un multiple de $p$ s'écrivant $d - 1 = pq$ avec $q \geq 2$.

- Premier cas : $d-1=p$

  $d$ et $p$ sont tous les deux des nombres premiers. Or aucun nombre premier sauf 2 n'est pair. La seule possibilité serait donc $d=3$ et $p=2$. Mais le nombre de Mersenne $M_2=2^2-1=3$ n'est pas composé. Donc il est exclu de cette étude. Donc $d-1=p$ est impossible.

- Deuxième cas : $d-1=pq$ avec $q\geq 2$ est la seule possibilité.

  On en déduit que l'indice $p$ du nombre de Mersenne composé $M_p$ divisible par $d$, divise $d-1$ et que le quotient $q$ vérifie $q\geq 2$.

  $p$ divise $d-1$ et le quotient $q\geq 2$ s'écrit $d-1=pq$ avec $q\geq 2$, c'est-à-dire $d=qp+1 \quad (q\geq 2)$.

d) D'après la question précédente 2)c), on a $d=qp+1 \quad (q\geq 2)$.
On a vu que l'étude porte sur les nombres de Mersenne $M_p$ avec $p$ premier et $p\geq 3$.
On en déduit que $d\geq 7$. Donc $d$ est premier et $d\geq 7$. Donc $d$ est impair.
De la relation $d=qp+1 \quad (q\geq 2)$ on déduit que $qp$ est pair. Comme $p$ est premier et $p\geq 3$ donc $p$ est impair. Donc $q$ est pair. On en déduit que $q=2k$ où $k$ est un entier naturel. Puisque $q\geq 2$, on a $k\geq 1$.
Conclusion : Si $M_p$ est composé alors pour chacun de ses diviseurs premiers $d$, il existe $k\in\mathbb{N}^*$ tel que :

$$d=2k\times p+1.$$

Donc les diviseurs premiers éventuels de $M_p$ sont à chercher parmi les nombres $2k\times p+1 \quad (k\in\mathbb{N}^*)$.

**Partie B:** ***Application à deux nombres de Mersenne $M_p$ avec p premier***

1) Le nombre de Mersenne $M_{19}=2^{19}-1=524287$
   a) $p=19$ est premier donc si $M_{19}$ est composé alors, d'après la partie A, ses diviseurs premiers $d$ sont à chercher parmi les nombres :

$$d=2k\times 19+1 \quad (k\in\mathbb{N}^*).$$
$$d=38k+1 \quad (k\in\mathbb{N}^*).$$

   b) $\sqrt{M_{19}}\approx 724{,}08$

Donc, si $M_{19}$ a des diviseurs premiers, au moins l'un d'eux est tel que $d\leq 724$.

$$38k+1\leq 724 \quad (k\in\mathbb{N}^*)$$
$$38k\leq 723 \quad (k\in\mathbb{N}^*)$$
$$k\leq 19{,}03 \quad (k\in\mathbb{N}^*)$$

Donc il y a 19 valeurs possibles pour $k$ et donc 19 diviseurs de la forme $d=38k+1 \quad (k\in\mathbb{N}^*)$ inférieurs à $\sqrt{M_{19}}$.

   c) On peut présenter ces trois cas dans un tableau :

| | | |
|---|---|---|
| $d=38k+1,\ k\geq 1$ | $d=38k+1,\ k\geq 1$ | $d=38k+1,\ k\geq 1$ |
| $d=38(3m+1)+1,\ 3m+1\geq 1$ | $d=38(5m+3)+1,\ 5m+3\geq 1$ | $d=38(7m+2)+1,\ 7m+2\geq 1$ |
| $d=114m+38+1,\quad 3m\geq 0$ | $d=190m+114+1,\quad 5m\geq -2$ | $d=266m+76+1,\quad 7m\geq -1$ |
| $d=114m+39,\quad m\geq 0$ | $d=190m+115,\quad m\geq 0$ | $d=266m+77,\quad m\geq 0$ |
| $d=3\times(38m+13)$ | $d=5\times(38m+23)$ | $d=7\times(38m+11)$ |
| $d$ est divisible par 3 | $d$ est divisible par 5 | $d$ est divisible par 7 |

Conclusion : Lorsque $k=3m+1$ ou $k=5m+3$ ou $k=7m+2$, $d$ n'est pas un diviseur premier de $M_p$.

d) On doit donc chercher un éventuel diviseur premier $d$ de $M_{19}$ parmi les nombres $d = 38k + 1 \quad (k \in \mathbb{N}^*)$, en se limitant aux valeurs de $k$ entières telles que $1 \leq k \leq 19$ et en enlevant toutes les valeurs de $k$ telles que :

| $k = 3m + 1, \ m \geq 0$ | $k = 5m + 3, \ m \geq 0$ | $k = 7m + 2, \ m \geq 0$ |
|---|---|---|
| $1, 4, 7, 10, 13, 16, 19$ | $3, 8, 13, 18$ | $2, 9, 16$ |

Donc, au final, il reste seulement les valeurs de $k$ soulignées à examiner :

$$1, 2, 3, 4, \underline{5}, \underline{6}, 7, 8, 9, 10, \underline{11}, \underline{12}, 13, \underline{14}, \underline{15}, 16, \underline{17}, 18, 19$$

Donc il reste sept valeurs de $k$, donc sept valeurs de $d$ éventuelles qui pourraient être des diviseurs premiers du nombre de Mersenne $M_{19}$.

On essaye donc de diviser $M_{19} = 524287$ successivement par les sept valeurs de $d$ correspondant à $k = 5, 6, 11, 12, 14, 15, 17$. Si aucune de ces valeurs de $d$ n'est un diviseur de $M_{19}$ alors $M_{19}$ est un nombre de Mersenne premier.

| $k$ | $d$ | $d$ divise $M_{19} = 524287$ |
|---|---|---|
| $5$ | $191$ | non |
| $6$ | $229$ | non |
| $11$ | $419$ | non |
| $12$ | $457$ | non |
| $14$ | $533$ (est composé) | non |
| $15$ | $571$ | non |
| $17$ | $647$ | non |

Conclusion : aucune des valeurs de $d$ ne divise $M_{19}$. On peut conclure que $M_{19}$ est premier.

2) Le nombre de Mersenne $M_{23} = 2^{23} - 1 = 8388607$

a) $p = 23$ est premier donc si $M_{23}$ est composé alors, d'après la question 2)d) de la partie A, ses diviseurs premiers $d$ sont à chercher parmi les nombres :

$$d = 2k \times 23 + 1 \quad (k \in \mathbb{N}^*).$$

La première valeur possible comme diviseur premier $d$ correspond à $k = 1$. Il faut donc commencer par essayer de diviser $M_{23}$ par $d = 47$.

b) On essaye donc de diviser $M_{23} = 8388607$ par $47$.
$d = 47$ divise $M_{23}$. On peut conclure que $M_{23}$ n'est pas premier.

## Exercice 5

1) Les termes de la suite $S$ pour $i$ allant de 0 à 4 sont les suivants :

| $i$ | $S_i$ |
|---|---|
| 0 | 4 |
| 1 | 14 |
| 2 | 194 |
| 3 | 37634 |
| 4 | 1416317954 |
| 5 | $2{,}005957\ 10^{18}$ |

On constate une croissance très rapide. A partir de $S_8$ la taille des nombres $S_i$ dépasse la capacité d'affichage de la calculatrice.

2) a) $R_i$ est le reste de la division de $S_i$ par $M_p$ donc $S_i \equiv R_i \quad (M_p)$.

On en déduit que ${S_i}^2 \equiv {R_i}^2 \quad (M_p)$ (relation (1))

$R_{i+1}$ est le reste de la division de $S_{i+1}$ par $M_p$ donc $S_{i+1} \equiv R_{i+1} \quad (M_p)$ (relation (2))

De plus $S_{i+1} \equiv S_i^2 - 2 \quad (M_p)$ donc, en utilisant la relation (1) on a : $S_{i+1} \equiv R_i^2 - 2 \quad (M_p)$

Et en utilisant la relation (2) on a finalement pour tout $i \geq 0$, $\boxed{R_i^2 - 2 \equiv R_{i+1} \quad (M_p)}$.

b) La formule de tableur =MOD($S_{i+1}$ ; $M_p$) donne le reste de la division euclidienne de $S_{i+1}$ par $M_p$.

Or, $S_{i+1} \equiv R_{i+1} \quad (M_p)$ (relation (2)) et comme $R_{i+1}$ désigne le reste de la division de $S_{i+1}$ par $M_p$ alors =MOD($S_{i+1}$ ; $M_p$) donne le reste $R_{i+1}$.

=MOD(${R_i}^2 - 2; M_p$) donne le reste de la division de ${R_i}^2 - 2$ par $M_p$.

Or, $\boxed{R_i^2 - 2 \equiv R_{i+1} \quad (M_p)}$ et comme $R_{i+1}$ désigne un reste d'une division par $M_p$, et donc vérifie $0 \leq R_{i+1} < M_p$, alors =MOD(${R_i}^2 - 2; M_p$) donne le reste $R_{i+1}$.

c) Il n'est pas possible de travailler avec les valeurs $S_i$ dans la feuille de calcul du tableur car la taille de ces nombres dépasse rapidement la capacité du tableur.

Au contraire, la deuxième formule =MOD(${R_i}^2 - 2; M_p$) ne fait appel qu'aux restes $R_i$ qui vérifient tous $0 \leq R_i < M_p$.

Donc, tant que les valeurs des nombres ${R_i}^2 - 2$ ne dépassent pas la capacité du tableur, ce qui est le cas pour $M_{19}$, alors la feuille de calcul affichera correctement les valeurs.

d) La feuille de calcul est la suivante :

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | **p=** | 3 | 5 | 7 | 11 | 13 | 17 | 19 |
| 2 | **Mp=** | 7 | 31 | 127 | 2047 | 8191 | 131071 | 524287 |
| 3 | | | | | | | | |
| 4 | **i** | **Ri** | **Ri** | **Ri** | **Ri** | **Ri** | **Ri** | **Ri** |
| 5 | 0 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| 6 | 1 | 0 | 14 | 14 | 14 | 14 | 14 | 14 |
| 7 | 2 | 5 | 8 | 67 | 194 | 194 | 194 | 194 |
| 8 | 3 | 2 | 0 | 42 | 788 | 4870 | 37634 | 37634 |
| 9 | 4 | 2 | 29 | 111 | 701 | 3953 | 95799 | 218767 |
| 10 | 5 | 2 | 2 | 0 | 119 | 5970 | 119121 | 510066 |
| 11 | 6 | 2 | 2 | 125 | 1877 | 1857 | 66179 | 386344 |
| 12 | 7 | 2 | 2 | 2 | 240 | 36 | 53645 | 323156 |
| 13 | 8 | 2 | 2 | 2 | 282 | 1294 | 122218 | 218526 |
| 14 | 9 | 2 | 2 | 2 | 1736 | 3470 | 126220 | 504140 |
| 15 | 10 | 2 | 2 | 2 | 510 | 128 | 70490 | 103469 |
| 16 | 11 | 2 | 2 | 2 | 129 | 0 | 69559 | 417706 |
| 17 | 12 | 2 | 2 | 2 | 263 | 8189 | 99585 | 307417 |
| 18 | 13 | 2 | 2 | 2 | 1616 | 2 | 78221 | 382989 |
| 19 | 14 | 2 | 2 | 2 | 1529 | 2 | 130559 | 275842 |
| 20 | 15 | 2 | 2 | 2 | 165 | 2 | 0 | 85226 |
| 21 | 16 | 2 | 2 | 2 | 612 | 2 | 131069 | 523263 |
| 22 | 17 | 2 | 2 | 2 | 1988 | 2 | 2 | 0 |
| 23 | 18 | 2 | 2 | 2 | 1432 | 2 | 2 | 524285 |
| 24 | 19 | 2 | 2 | 2 | 1575 | 2 | 2 | 2 |
| 25 | 20 | 2 | 2 | 2 | 1706 | 2 | 2 | 2 |
| 26 | 21 | 2 | 2 | 2 | 1647 | 2 | 2 | 2 |
| 27 | 22 | 2 | 2 | 2 | 332 | 2 | 2 | 2 |
| 28 | 23 | 2 | 2 | 2 | 1731 | 2 | 2 | 2 |
| 29 | 24 | 2 | 2 | 2 | 1598 | 2 | 2 | 2 |
| 30 | 25 | 2 | 2 | 2 | 993 | 2 | 2 | 2 |
| 31 | 26 | 2 | 2 | 2 | 1440 | 2 | 2 | 2 |
| 32 | 27 | 2 | 2 | 2 | 2034 | 2 | 2 | 2 |
| 33 | 28 | 2 | 2 | 2 | 167 | 2 | 2 | 2 |
| 34 | 29 | 2 | 2 | 2 | 1276 | 2 | 2 | 2 |
| 35 | 30 | 2 | 2 | 2 | 809 | 2 | 2 | 2 |

- Pour $p = 11$ aucun reste $R_i$ de la division de $S_i$ par $M_p$ n'est nul. On vérifie avec le programme ESTPREM sur la calculatrice que le nombre de Mersenne correspondant $M_{11} = 2047$ est composé.

3) On vérifie avec le programme ESTPREM sur la calculatrice que les nombres de Mersenne $M_3 = 7$ , $M_5 = 31$, $M_7 = 127$, $M_{13} = 8191$, $M_{17} = 131071$ , $M_{19} = 524287$ sont effectivement premiers.

a) On peut conjecturer que le rang $r$ du reste $R_i$ nul, pour les nombres $M_p$ qui sont premiers, vérifie $r = p - 2$.

b) A partir du rang $r + 2 = p$ on peut conjecturer que tous les restes $R_i$ sont égaux à 2.

c) Par définition du rang $r$, on a $R_r = 0$.

D'après la question 2)a), on sait que $R_{r+1} \equiv {R_r}^2 - 2 \quad (M_p)$. Donc $R_{r+1} \equiv 0^2 - 2 \quad (M_p)$.
De même on sait que $R_{r+2} \equiv {R_{r+1}}^2 - 2 \quad (M_p)$. Donc $R_{r+2} \equiv (-2)^2 - 2 \quad (M_p)$ c'est-à-dire $R_{r+2} \equiv 2 \quad (M_p)$.

Montrons par récurrence que la proposition $P(i)$ : « $R_{r+i} \equiv 2 \quad (M_p)$ » est vraie pour tout entier $i \geq 2$.

- Initialisation : On vient d'établir que $R_{r+2} \equiv 2 \quad (M_p)$. Donc la proposition $P(i)$ est vraie pour $i = 2$.
- Hérédité : Supposons que pour un certain entier $k \geq 2$, on ait $R_{r+k} \equiv 2 \quad (M_p)$.

D'après la question 2)a), on sait que $R_{r+k+1} \equiv {R_{r+k}}^2 - 2 \quad (M_p)$ et comme par hypothèse de récurrence on suppose que $R_{r+k} \equiv 2 \quad (M_p)$ donc $R_{r+k+1} \equiv 2^2 - 2 \quad (M_p)$. Donc $R_{r+k+1} \equiv 2 \quad (M_p)$.

- Conclusion : La proposition « $R_{r+i} \equiv 2 \quad (M_p)$ » est vraie pour tout $i \geq 2$.

4) Propriété de Lucas – Lehmer

a) On complète l'algorithme :

Saisir $p$ ($p$ doit être premier, supérieur ou égal à 3)
$R$ prend la valeur 4
$M$ prend la valeur $2^p - 1$
Pour $k$ allant de 1 à $p - 2$
  $R$ prend la valeur *reste de la division de* $R^2 - 2$ *par* $M$
Fin pour
Si $R = 0$ alors
  Afficher **M EST PREMIER**.....
  Sinon
  Afficher **M EST COMPOSE**.....
Fin si

b) Le programme LLT dans la calculatrice peut être :

| Texas Instruments TI82 - TI 83 | Casio Graph 35+ USB |
|---|---|
| Prompt P | "P="?→P |
| 4→R | 4→R |
| 2^P-1→M | 2^P-1→M |
| For(I,1,P-2) | For 1→I To P-2 |
| R²-2→A | R²-2→A |
| A-partEnt(A/M)*M→R | A-Intg (A÷M)×M→R |
| End | Next |
| If R=0 | If R=0 |
| Then | Then |
| Disp "M EST PREMIER" | "M EST PREMIER"◢ |
| Else | Else |
| Disp "M EST COMPOSE" | "M EST COMPOSE"◢ |
| End | IfEnd |

On teste le programme :

- Pour $P = 19$, le programme affiche « M est premier »
- Pour $P = 23$, le programme affiche « M est composé »

ce qui est le résultat attendu. Donc le programme semble fonctionner correctement.

c) Pour $P = 107$, (on vérifie que 107 est bien un nombre premier) le programme affiche « M est premier ».