Partie I Etude du reste de la division euclidienne de 2^n-1 par 2^m-1

1. Ouvrir une feuille de calcul.(Excel ou OpenOffice)
   Enregistrer cette feuille de calcul dans votre zone personnelle, dans un répertoire :
   P :/Maths/Specialite/TP
   et lui donner le nom de :
   EtudeNombreMersenne01.xls ou **EtudeNombreMersenne01.ods**
2. En utilisant la feuille de calcul, afficher deux listes de 30 nombres entiers aléatoires entre 1 et 40. On note n les nombres de la premieres liste et m ceux de la deuxième.
3. Pour toutes les valeurs de n et m, comparer le reste de la division euclidienne de n par m et le reste de la division euclidienne de 2^n-1 par 2^m-1.
   Quelle conjecture peux-tu faire ? (✺)
4. Démonstration :
   (a) $n \in \mathbb{N}$ et $m \in \mathbb{N}$, donc il existe $(q,r) \in \mathbb{N}^2$ tels que $n = mq + r$ avec $0 \leq r < m$
   et $2^n - 1 = 2^{mq+r} - 1 = 2^{mq} \times 2^r - 1 = (2^{mq} - 1) \times 2^r + 2^r - 1$
   (b) On reconnaît la somme des termes d'une suite géométrique de raison 2^m et de premier terme 1.
   Donc :
   $2^{m(q-1)} + 2^{m(q-2)} + \ldots 2^m + 1 = \dfrac{1-(2^m)^q}{1-2^m} = \dfrac{1-2^{mq}}{1-2^m}$
   (c) D'après la question précédente :
   $2^{mq} - 1 = (2^{m(q-1)} + 2^{m(q-2)} + \ldots 2^m + 1)(2^m - 1)$
   donc $2^n - 1 = \left[(2^{m(q-1)} + 2^{m(q-2)} + \ldots 2^m + 1) \times 2^r\right](2^m - 1) + (2^r - 1)$
   En posant $q = (2^{m(q-1)} + 2^{m(q-2)} + \ldots 2^m + 1) \times 2^r$ alors :
   $2^n - 1 = q \times (2^m - 1) + (2^r - 1)$
   or $0 < m \Rightarrow 0 \leq 2^r - 1 < 2^m - 1$ car $f : x \mapsto 2^x - 1 = e^{xln(2)} - 1$ est strictement croissante sur $\mathbb{R}^+$.
   donc
   $\boxed{2^r - 1 \text{ est le reste de la division euclidienne de } 2^n - 1 \text{ par } 2^m - 1}$.

Partie II Etude du $PGCD(2^n-1; 2^m-1)$.

1. Sur la même feuille de calcul que précédemment.
   Pour toutes les valeurs de n et m, faire apparaître une relation
   entre $PGCD(2^n-1; 2^m-1)$ et $PGCD(n;m)$ (✺)
2. En utilisant la Partie I et l'algorithme d'Euclide, démontrons cette conjecture.
   (a) On note r_1, r_2 $\ldots r_k$ les restes successifs dans l'algorithme d'euclide de la division de n par m.
   D'après la question précédente, on peut dresser le tableau ci-dessous :

	Division de n par m	Division de 2^n-1 par 2^m-1
(1)	$n = q_1 m + r_1$	$2^n - 1 = q'_1(2^m - 1) + (2^{r_1} - 1)$
(2)	$m = q_2 r_1 + r_2$	$2^m - 1 = q'_2(2^{r_1} - 1) + (2^{r_2} - 1)$
	$\vdots$	$\vdots$
(k)	$r_{k-1} = q_{k-1} r_{k-2} + r_k$	$2^{r_{k-1}} - 1 = q'_{k-1}(2^{r_{k-2}} - 1) + (2^{r_k} - 1)$

   donc $2^{r_1}-1$, $2^{r_2}-1$, $\ldots$,$2^{r_k}-1$ sont les restes successifs de l'algorithme d'euclide pour la division de 2^n-1 par 2^m-1.
   (b) Le dernier reste non nul des divisions euclidienne (dans l'algorithme d'Euclide) est le PGCD
   donc $PGCD(2^n-1; 2^m-1) = 2^{PGCD(n;m)} - 1$

Partie III Etude de 2^n-1 et 2^m-1 si m et n sont premiers entre eux.

1. Quelle conjecture peux-tu faire si m et n sont premiers entre eux ? (✺)
2. Si m et n sont étrangers, alors $PGCD(n;m) = 1$ donc $PGCD(2^n-1; 2^m-1) = 1$
   donc 2^n-1 et 2^m-1 sont étrangers ou premiers entre eux.