EULER (mathématicien suisse, 1707-1783) ayant démontré qu'il y a une infinité de nombres premiers, de nombreux mathématiciens, et lui en tête, ont cherché des expressions simples donnant des nombres premiers. Sans parvenir à une formule générale, ils ont néanmoins découvert des « familles » de nombres premiers.

1° EULER

Nombres de la forme $n^2 - n + 41$

On montre que, pour tous les entiers n allant de 0 à 20, $n^2 - n + 41$ est un nombre premier.

- Vérifier cette formule pour tous les entiers n de 0 à 20.
- Montrer que pour $n = 41$, le nombre $n^2 - n + 41$ n'est pas premier.

2° NOMBRES DE MERSENNE (savant français, correspondant de Descartes, Pascal, Fermat... 1588-1648)

Nombres de la forme $2^n - 1$, où n est un nombre premier

- Vérifier que cette formule donne des nombres premiers, en prenant pour n les premiers nombres premiers.
- Quelle est la première valeur de n qui ne donne pas un nombre premier par cette formule ?

On ne sait pas prouver que:

- les nombre de Mersenne premiers sont en nombre infini
- les nombres de Mersenne composés, ayant un exposant premier, sont en nombre infini

On sait aussi que

- si " M_p " est premier, alors " p " l'est aussi.

- si p est composé (non premier) alors M_p est composé

$2^{3021377} - 1$ est le 37^e nombre premier de Mersenne connu. en 1998.

$2^{20996011} - 1$ est le 40^{ième} nombre premier de Mersenne connu en 2003 (Cela a peut-être changé encore.)

3° NOMBRES DE FERMAT (mathématicien français 1601-1665) :

nombres de la forme $2^{2^n} + 1$, où n est un entier naturel

- Calculer les nombres obtenus avec n entier allant de 0 à 3.
- En revanche, montrer que la valeur $n = 5$ donne un nombre divisible par 641.

Pour en savoir plus consulter : <http://membres.lycos.fr/villemingerard/>

Remarque . **Intérêt des grands nombres premiers**

Pour sécuriser la transmission des informations, on crypte les données. Il existe plusieurs techniques de cryptage, mais actuellement le système de cryptage RSA est très utilisé.

Principe

On crypte les données à l'aide d'un entier n très grand appelé la clef.

Cet entier sert uniquement à coder, on peut donc la diffuser sans danger.

C'est ce qu'on appelle une clef publique. Seul le créateur du nombre n peut décrypter les données.

En effet, avec le système RSA, n est le produit de deux nombres premiers très grands (donc $n = a \times b$).

C'est a et b qui permettent de décrypter les messages. La fiabilité de ce système repose sur la difficulté de décomposer un entier en produit de facteur premier (un ordinateur peut chercher plusieurs mois pour trouver a et b connaissant n , car les nombres sont très grands).

La connaissance des grands nombres premiers est alors très convoitée...