Club MATH

Centre informatique pédagogique (CIP)
Case Postale 172
1211 GENEVE 3
Tél. (022) 318.05.30
Responsable:
Raymond Morel

Supplément à la lettre nº 8

Lundi 13 janvier 1992 à 17 h.

Voulez-vous inscrire votre nom dans les annales mathématiques ?

Présentation: Bernard Vuilleumier

Il a fallu plus de deux mille ans pour dresser cette liste

Voici une liste de trente et un nombres premiers très particuliers:
2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091.

Il a fallu plus de deux mille ans pour dresser cette liste, mais les six derniers nombres ont été découverts entre 1980 et 1990. Si vous trouvez le suivant, vous pourrez calculer un nombre premier supérieur au plus grand nombre de Mersenne premier connu à ce jour (au 1er octobre 1990) qui est $2^{216091} - 1$. Vous serez alors, pour un temps, le découvreur du plus grand nombre premier connu! Les nombres premiers p de cette liste sont en effet tels que:

Chacun des nombres de cette liste détermine un nombre premier

$2^p - 1$ est un nombre premier

Les nombres de la forme $2^q - 1$ sont appelés nombres de Mersenne. La liste des nombres ci-dessus n'étant pas bien longue, les nombres de Mersenne premiers ne sont donc pas très fréquents. Leur intérêt réside dans le fait qu'il est aisé d'écrire un algorithme s'appuyant sur le théorème de Lucas-Lehmer et permettant de tester s'ils sont premiers ou non. Ce théorème établit qu'un nombre de Mersenne M_q (de la forme $M_q = 2^q - 1$) est premier si et seulement si, pour la suite $x_1 = 4$, $x_{n+1} = x_n^2 - 2$, le reste de la division de x_{q-1} par M_q est égal à 0.

Dans certains cas, il est possible de tester rapidement si un nombre est premier

• Comment s'y prendre

La première idée qui vient à l'esprit d'un utilisateur de *Mathematica* pour tester un nombre de Mersenne M_q, c'est de définir la suite x_n, de calculer le terme x_{q-1} et d'examiner le reste de la division de ce terme par M_q:

```
x[1]=4
x[n_]:=x[n-1]^2-2
Mod[x[q-1],2^q-1]
```

La première idée n'est pas toujours la bonne !

Cette façon de procéder n'est pas la bonne pour deux raisons:

1º le temps de calcul devient très vite prohibitif (6 secondes pour q=16, 52 secondes pour q=17, 205 secondes pour q=18, ...)

2º même si vous êtes patient, il se produira, pour des valeurs élevées de q, un dépassement de la profondeur de récursion autorisée par *Mathematica*.

Nous allons donc utiliser une boucle plutôt qu'une relation de récurrence pour calculer le terme x_{q-1}.

```
x=4
Do[x=x^2-2,{q-2}]
```

N.B. Le terme x_1 étant donné, le premier passage dans la boucle fournit x_2. Il faut donc effectuer la boucle q-2 fois pour obtenir le terme de rang q-1.

Imprimons quelques termes pour examiner leur croissance:

```
q=7;
x=4
Do[Print[x=x^2-2],{q-2}]
```

Les termes de la suite croissent très vite

```
4
14
194
37634
1416317954
2005956546822746114
```

Il est plus rapide de travailler avec des petits nombres qu'avec des grands !

Comme seul le reste de la division du terme x_{q-1} par M_q nous intéresse, nous pouvons effectuer la division par M_q à chaque passage plutôt que d'attendre la fin de la boucle avant de l'effectuer. Nous limitons ainsi considérablement la taille des termes et gagnons en rapidité d'exécution:

```
q=2203;
x=4;
Do[x=Mod[x^2-2,2^q-1],{q-2}]
If[x!=0,Print["Mq est composé"],
Print["Mq est premier"]]
```

Sur ma machine favorite, le test pour M_{2203} dure 2' 54". Et sur la vôtre ?

Pour en savoir plus

Lehmer, D. H., *Journal of the London Mathematical Society, vol. 10,* 1935, pp. 162-165.
Hardy, G, Wright, E. - *An Introduction to the Theory of Numbers.* - New York: Oxford University Press, 1979.
Ribenboim, P. - *The Book of Prime Number Records.* - Springer-Verlag, 1988.

Prochaine réunion: lundi 3 février 1992 à 17 h.