Les nombres de Fermat

Livre Math'x TS spécialité édition 2012

Exercice 9 Nombres de Fermat

En 1640, Fermat annonce qu'il est persuadé que les nombres $F_n = 2^{2^n} + 1$ sont premiers :
« Je n'en ai pas la démonstration exacte mais j'ai exclu une si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières qui établissent ma pensée que j'aurais peine à me dédire. »

Attention à l'écriture. On devrait plutôt écrire $F_n = 2^{\left(2^n\right)} + 1$.

1°) Calculer F_0, F_1, F_2, F_3 et vérifier l'affirmation de Fermat. (On considérera comme connus les nombres premiers inférieurs à 20).

2°) Calculer F_4 à la calculatrice ou avec un logiciel de calcul. Est-il premier ?

3°) Quel est le plus petit facteur premier de F_5 ?

Point Histoire

Pierre de Fermat (1601 – 1665) fut conseiller au Parlement de Toulouse. Amateur de mathématiques, il les étudie pendant ses loisirs. Ses travaux concernent principalement les courbes, l'arithmétique et le calcul des probabilités qu'il développe dans une correspondance avec Pascal.

Même si l'on n'a pas démontré qu'il n'existe pas d'autres nombres de Fermat premiers, on ne connaît pour l'instant que 5 nombres premiers de la forme $2^{2^n} + 1$ pour *n* de 0 à 4… La difficulté vient ensuite de la taille des nombres F_n même pour de petites valeurs de *n*.

Euler a montré que F_5 est composé avec : $F_5 = 641 \times 6700417$.

Puis en 1880, Lamy prouve que $F_6 = 274\,177 \times 67280421310721$.

On a depuis démontré que F_n est composé pour $5 \leqslant n \leqslant 32$.

Les nombres de Fermat premiers ont une application en géométrie. En effet Karl Friedrich Gauss (1777-1855) a démontré qu'un polygone régulier à *n* côtés est constructible à la règle et au compas si et seulement si :

$n = 2^k \times p_1 \times ... \times p_r$ avec p_i un nombre premier de Fermat.

Solution :

$F_1 = 5$, $F_2 = 17$, $F_3 = 557$, $F_4 = 65537$, $F_5 = 4\ 294\ 967\ 297$

Livre Indice TS spécialité mathématiques Programme 2012 page 15

Les nombres de Fermat

Objectif : Découvrir des nombres historiques

En 1640, le mathématicien Pierre de Fermat pensait que les nombres $F_n = 2^{2^n} + 1$ avec $n \in \mathbb{N}$ (que l'on appelle aujourd'hui les nombres de Fermat) sont tous premiers.

1°) Vérifier avec une calculatrice (en utilisant par exemple le programme du problème précédent) que les entiers F_j sont premiers pour $0 \leqslant j \leqslant 4$.

2°) Il faut attendre 1732 pour avoir une preuve (apportée par le mathématicien Leonhard Euler) du caractère non premier de F_5.

Aujourd'hui, l'instruction du logiciel **Xcas** [factoriser_entier(2^(2^5)+1)] ou l'instruction [factor(2^(2^5)+1)] avec le logiciel **Derive** retourne de façon quasi instantanée la factorisation de F_6.

factoriser_entier(2^(2^6)+1)
2741177.67280421310721

Le point désigne une multiplication.

Aujourd'hui encore, on ne sait factoriser que peu de nombres de Fermat. Pour comprendre cela, on peut commencer par se donner une idée de la taille de ces nombres. En supposant que l'on écrive 5 chiffres par seconde, et sachant que F_{30} a plus de 10^8 chiffres, combien de temps faudra-t-il pour écrire un tel entier ?

3°) Vérifier que tous les nombres de Fermat sont impairs.

4°) Démontrer, par récurrence, que pour tout entier $n \geqslant 1$, on a : $F_0 F_1 ... F_{n-1} = F_n - 2$.

5°) Déduire des deux questions précédentes que si d est un diviseur commun à deux nombres de Fermat, alors $d = 1$.

6°) Sachant que tout entier admet au moins un facteur premier, déduire de ce qui précède une démonstration de l'infinité des nombres premiers.

Pascal Fermat mentionne ces nombres dans une lettre à Pascal datant de … .

L'étude de ces nombres s'inscrit dans la quête des nombres premiers relancée avec l'avènement de l'informatique et l'explosion du numérique au XX^{e} siècle.

Livre Odyssée page 75 :

Une réciproque ?

a) Énoncer la contraposée de la propriété démontrée à la question 2°) c).
b) Énoncer la réciproque de la propriété énoncée à la question 3°) a).
c) Vérifier que F_5 est divisible par 641.
d) Que peut-on penser de la propriété de la propriété énoncée) la question 3°) b) ?

Évidemment la propriété espérée par Pierre de Fermat est celle énoncé à la question 3°) b). « Si *m* est une puissance de 2, alors 2^m+1 est premier ». Cette propriété permettrait de générer une infinité de nombres premiers à l'aide de cette formule.
Malheureusement, il ne put démontrer cette propriété ; en effet, F_5 est un contre-exemple qui lui aurait évité bien des recherches.
En 1640, Pierre de Fermat reconnaît ses difficultés dans une lettre adressée à Bernard Frénicle de Bessy :
« *je n'ai pu encore démontrer nécessairement la vérité de cette proposition* ».
Toutefois, la propriété « Si *m* n'est pas une puissance de 2, alors 2^m+1 n'est pas premier » lui a permis d'imaginer ces nombres de la forme $2^{2^n}+1$ ce qui n'est pas si mal…
Les quatre siècles de recherche qui ont suivi, ont révélé qu'aucun d'eux ne l'est pour *n* allant de 5 à 32.
Mais l'incertitude reste pour *n* supérieur à 32…

Utilisation pour les polygones constructibles à la règle et au compas