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

## Correction de l’activité 2. Nombres de Fermat (4 exercices)

**Exercice 1 : *Présentation générale des nombres de Fermat***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre de Fermat |  | Premier ? | Méthode |
| 0 |  |  | Oui | Nombre premier connu |
| 1 |  |  | Oui | Nombre premier connu |
| 2 |  |  | Oui | Nombre premier connu |
| 3 |  |  | Oui | Algorithme TESTB (en 2s) |
| 4 |  |  | Oui | Algorithme TESTB (en 4s) |
| 5 |  |  | Non | Algorithme TESTB (en 10s)  (L'algorithme DIVISPRE donne comme plus petit diviseur premier ). |
| 6 |  |  | Non? | Algorithme TESTB (en 1s) |

* Dans le dernier cas, le temps d'exécution de l'algorithme est suspect, car est impair et l'algorithme n'a pas pu conclure par une analyse de la parité. Il s'agit plutôt d'une confusion avec un autre nombre que , celui-ci étant trop grand (20 chiffres significatifs) pour la calculatrice. Cela est confirmé en lançant l'algorithme DIVISPRE !
* Pour ce type de calcul, il faut s'assurer que la machine qui exécute le programme de l'algorithme puisse manipuler des nombres avec suffisamment de chiffres significatifs.
* Une solution est d'utiliser l'outil de calcul en ligne sur le serveur WIMS <http://wims.unice.fr/wims> dans l'outil "Primes", le factoriseur d'entiers. Effectivement est factorisable.

**Exercice 2 : *Deux relations de récurrence vérifiées par les nombres de Fermat***

1. On part de la définition des nombres de Fermat. Pour tout entier naturel :
2. Démontrons par récurrence :

* Initialisation :

Pour , la proposition s'écrit .

Puisque et alors la proposition est vraie au premier rang.

* Hérédité :

Supposons que pour un entier fixé, on ait (c'est l'hypothèse de récurrence).

Exprimons de façon à utiliser l'hypothèse de récurrence.

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

La proposition est héréditaire.

* Conclusion :

Pour tout :

**Exercice 3 : *L’infinitude des nombres premiers démontrée avec les nombres de Fermat***

1. On part de la définition des nombres de Fermat. Pour tout entier naturel :

Or

Donc

pour tout . Donc tous les nombres de Fermat sont impairs.

1. Si divise alors il existe un entier tel que et donc

s'écrit

Si divise aussi alors il existe un entier tel que et donc la relation donnée (et démontrée dans l'exercice 2)

Pour tout :

s'écrit

Pour tout :

est un entier donc divise 2.

Cela est contradictoire avec la supposition .

Conclusion : Le seul diviseur commun que peuvent avoir deux nombres de Fermat quelconques est 1 ou 2. Mais comme aucun nombre de Fermat n'est pair, deux nombres de Fermat ont toujours comme PGCD 1.

1. On déduit directement da la question 2) que deux nombres de Fermat distincts sont premiers entre eux.
2. a) D'après la question 3) on sait que est premier avec tous les nombres . Donc n'a aucun des diviseurs contenus dans l'ensemble des diviseurs premiers .

Comme a au moins un diviseur premier, alors il y a au moins un élément de plus dans l'ensemble des diviseurs premiers que dans l'ensemble des diviseurs premiers .

* 1. Comme le nombre de nombres de Fermat est infini, on en déduit que le nombre de nombres premiers est aussi infini.

**Exercice 4 : *A partir de n = 2, Fn a comme chiffre des unités 7***

1. On a pour tout ,

Donc :

et

Formons progressivement la somme :

Conclusion : Pour tout entier naturel ,

1. Démontrons par récurrence :

* Initialisation :

Pour , la proposition s'écrit a pour chiffre des unités .

Puisque alors la proposition est vraie au premier rang.

* Hérédité :

Supposons que pour un entier fixé, on ait (c'est l'hypothèse de récurrence).

Etablissons une relation de congruence entre et de façon à utiliser l'hypothèse de récurrence.

D'après la question 1) on a :

Donc :

Comme alors :

et

Ainsi en faisant la somme membre à membre :

Ou encore :

Finalement :

La proposition est héréditaire.

* Conclusion :

Pour tout :

Tous les nombres de Fermat, à partir de ont donc pour chiffre des unités .