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*

n	Nombre de Fermat F_n		Premier ?	Méthode
0	$F_0 = 2^1 + 1$	$F_0 = 3$	Oui	Nombre premier connu
1	$F_1 = 2^2 + 1$	$F_1 = 5$	Oui	Nombre premier connu
2	$F_2 = 2^4 + 1$	$F_2 = 17$	Oui	Nombre premier connu
3	$F_3 = 2^8 + 1$	$F_3 = 257$	Oui	Algorithme TESTB (en 2s)
4	$F_4 = 2^{16} + 1$	$F_4 = 65\,537$	Oui	Algorithme TESTB (en 4s)
5	$F_5 = 2^{32} + 1$	$F_5 = 4\,294\,967\,297$	Non	Algorithme TESTB (en 10s) (L'algorithme DIVISPRE donne comme plus petit diviseur premier 641).
6	$F_6 = 2^{64} + 1$	$F_6 = 18\,446\,744\,073\,709\,551\,617$	Non?	Algorithme TESTB (en 1s)

- Dans le dernier cas, le temps d'exécution de l'algorithme est suspect, car F_6 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 $F_6 = 2^{64} + 1$, 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 F_6 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 n :

$F_n = 2^{2^n} + 1$

$F_n - 1 = 2^{2^n}$

$(F_n - 1)^2 = \left(2^{2^n}\right)^2$

$(F_n - 1)^2 = 2^{2^n \times 2}$

$(F_n - 1)^2 = 2^{2^{n+1}}$

$(F_n - 1)^2 = \left(2^{2^{n+1}} + 1\right) - 1$

$(F_n - 1)^2 = F_{n+1} - 1$

2) Démontrons par récurrence :

- Initialisation :

Pour $n = 1$, la proposition s'écrit $F_0 = F_1 - 2$.

Puisque $F_0 = 3$ et $F_1 = 5$ alors la proposition est vraie au premier rang.

- Hérédité :

Supposons que pour un entier $k \in \mathbb{N}^*$ fixé, on ait $F_0 \times F_1 \times \ldots \times F_{k-1} = F_k - 2$ (c'est l'hypothèse de récurrence).

Exprimons $F_0 \times F_1 \times \ldots \times F_{k-1} \times F_k$ de façon à utiliser l'hypothèse de récurrence.

$$F_0 \times F_1 \times \ldots \times F_{k-1} \times F_k = (F_0 \times F_1 \times \ldots \times F_{k-1}) \times F_k$$

$$F_0 \times F_1 \times \ldots \times F_{k-1} \times F_k = (F_k - 2) \times F_k$$

$$F_0 \times F_1 \times \ldots \times F_{k-1} \times F_k = {F_k}^2 - 2F_k$$

$$F_0 \times F_1 \times \ldots \times F_{k-1} \times F_k = {F_k}^2 - 2F_k + 1 - 1$$

$$F_0 \times F_1 \times \ldots \times F_{k-1} \times F_k = (F_k - 1)^2 - 1$$

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

$$F_0 \times F_1 \times \ldots \times F_{k-1} \times F_k = F_{k+1} - 1 - 1$$

$$F_0 \times F_1 \times \ldots \times F_{k-1} \times F_k = F_{k+1} - 2$$

La proposition est héréditaire.

- Conclusion :

Pour tout $n \in \mathbb{N}^*$: $F_0 \times F_1 \times \ldots \times F_{n-1} = F_n - 2$

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 n :

$F_n = 2^{2^n} + 1$

Or $2^{2^n} \equiv 0 \quad (2)$

Donc $2^{2^n} + 1 \equiv 1 \quad (2)$

$F_n \equiv 1 \quad (2)$ pour tout $n \in \mathbb{N}$. Donc tous les nombres de Fermat sont impairs.

2) Si d divise F_k alors il existe un entier q tel que $dq = F_k$ et donc

$$F_0 \times F_1 \times \ldots \times F_k \times \ldots \times F_{n-1}$$

s'écrit $F_0 \times F_1 \times \ldots \times dq \times \ldots \times F_{n-1}$

Si d divise aussi F_n alors il existe un entier q' tel que $dq' = F_n$ et donc la relation donnée (et démontrée dans l'exercice 2)

$$\text{Pour tout } n \in \mathbb{N}^* : F_0 \times F_1 \times \ldots \times F_{n-1} = F_n - 2$$

s'écrit

$$\text{Pour tout } n \in \mathbb{N}^* : F_0 \times F_1 \times \ldots \times dq \times \ldots \times F_{n-1} = dq' - 2$$

$$F_0 \times F_1 \times \ldots \times dq \times \ldots \times F_{n-1} = dq' - 2$$

$$2 = dq' - (F_0 \times F_1 \times \ldots \times dq \times \ldots \times F_{n-1})$$

$$2 = d[q' - (F_0 \times F_1 \times \ldots \times q \times \ldots \times F_{n-1})]$$

$[q' - (F_0 \times F_1 \times \ldots \times q \times \ldots \times F_{n-1})]$ est un entier donc d divise 2.
Cela est contradictoire avec la supposition $d \geq 3$.

<u>Conclusion :</u> 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.

3) On déduit directement da la question 2) que deux nombres de Fermat distincts sont premiers entre eux.

4) a) D'après la question 3) on sait que F_n est premier avec tous les nombres $F_0, F_1, \ldots, F_{n-1}$. Donc F_n n'a aucun des diviseurs contenus dans l'ensemble des diviseurs premiers E_{n-1}.

Comme F_n a au moins un diviseur premier, alors il y a au moins un élément de plus dans l'ensemble des diviseurs premiers E_n que dans l'ensemble des diviseurs premiers E_{n-1}.

b) 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, F_n a comme chiffre des unités 7*

1) On a pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$

Donc :

$F_{k+1} = 2^{2^{k+1}} + 1$ et $F_k = 2^{2^k} + 1$

Formons progressivement la somme ${F_k}^2 - 2F_k + 2$:

$$
\begin{aligned}
{F_k}^2 &= \left(2^{2^k} + 1\right)^2 \\
{F_k}^2 &= \left(2^{2^k}\right)^2 + 2 \times 2^{2^k} + 1 \\
{F_k}^2 &= 2^{2 \times 2^k} + 2 \times 2^{2^k} + 1 \\
{F_k}^2 - 2F_k &= 2^{2 \times 2^k} + 2 \times 2^{2^k} + 1 - 2\left(2^{2^k} + 1\right) \\
{F_k}^2 - 2F_k &= 2^{2 \times 2^k} + 2 \times 2^{2^k} + 1 - 2 \times 2^{2^k} - 2 \\
{F_k}^2 - 2F_k &= 2^{2 \times 2^k} - 1 \\
{F_k}^2 - 2F_k + 2 &= 2^{2 \times 2^k} + 1 \\
{F_k}^2 - 2F_k + 2 &= 2^{2^{k+1}} + 1
\end{aligned}
$$

Conclusion : Pour tout entier naturel k, $F_{k+1} = F_k^2 - 2F_k + 2$

2) Démontrons par récurrence :

- Initialisation :

Pour $n = 2$, la proposition s'écrit F_2 a pour chiffre des unités 7.

Puisque $F_2 = 17$ alors la proposition est vraie au premier rang.

- Hérédité :

Supposons que pour un entier $k \geq 2$ fixé, on ait $F_k \equiv 7 \quad (10)$ (c'est l'hypothèse de récurrence).

Etablissons une relation de congruence entre F_{k+1} et F_k de façon à utiliser l'hypothèse de récurrence.

D'après la question 1) on a : $F_{k+1} = F_k^2 - 2F_k + 2$

Donc : $F_{k+1} \equiv F_k^2 - 2F_k + 2 \quad (10)$

Comme $F_k \equiv 7 \quad (10)$ alors : ${F_k}^2 \equiv 49 \quad (10)$

$$ {F_k}^2 \equiv 9 \quad (10) $$

et $-2F_k + 2 \equiv -14 + 2 \quad (10)$

$$ -2F_k + 2 \equiv -12 \quad (10) $$

Ainsi en faisant la somme membre à membre : ${F_k}^2 - 2F_k + 2 \equiv -3 \quad (10)$

Ou encore : ${F_k}^2 - 2F_k + 2 \equiv 7 \quad (10)$

Finalement : $F_{k+1} \equiv 7 \quad (10)$

La proposition est héréditaire.

- Conclusion :

$$ \text{Pour tout } n \geq 2 : F_n = 7 \quad (10) $$

Tous les nombres de Fermat, à partir de F_2 ont donc pour chiffre des unités 7.