Corrigé du DM 12

Les nombres de Fermat

1. Introduction des nombres de Fermat :

a) Soient a et n deux entiers naturels. Une identité remarquable donne :

$$a^{2n+1}+1 = a^{2n+1}-(-1)^{2n+1} = (a-(-1))\sum_{j=0}^{2n} a^k(-1)^{2n-k} = (a+1)\sum_{j=0}^{2n} a^k(-1)^{2n-k}$$

Ainsi, $\boxed{a+1 \text{ divise } a^{2n+1}+1.}$

Autre approche : $a \equiv -1\ [a+1] \quad \Rightarrow \quad a^{2n+1} \equiv (-1)^{2n+1} \equiv -1\ [a+1] \quad \Rightarrow \quad a^{2n+1}+1 \equiv 0\ [a+1]$

b) Soit $n = k2^p$, où k naturel impair et p naturel, alors :

$$2^n+1 = \left(2^{2^p}\right)^k + 1$$

Ainsi, d'après **??**, $\boxed{\text{pour } a = 2^{2^p}, \text{ il vient que } 2^{2^p}+1 \text{ divise } 2^n+1.}$

c) Procédons par contraposition. Si q n'est pas un puissance de 2 alors il existe k impair et p un entier naturel tel que $q = k2^p$. Ainsi, d'après **??**, 2^q+1 est composé.

Ainsi, $\boxed{2^q+1 \text{ est premier implique que } q \text{ est une puissance de 2.}}$

2. Les nombres de Fermat sont premiers entre eux deux à deux (théorème de Goldbach) :

a) Soit $(n,k) \in \mathbb{N}\times\mathbb{N}^*$,

$$\begin{aligned} F_{n+k}-2 &= 2^{2^{n+k}}-1 = 2^{2^{n+1}2^{k-1}}-1 = \left(2^{2^{n+1}}\right)^{2^{k-1}}-1 \\ &= \left(2^{2^{n+1}}-1\right)\sum_{j=0}^{2^{k-1}}\left(2^{2^{n+1}}\right)^j = \left(\left(2^{2^n}\right)^2-1\right)\sum_{j=0}^{2^{k-1}}\left(2^{2^{n+1}}\right)^j \\ &= \left(2^{2^n}-1\right)\big(\underbrace{2^{2^n}+1}_{=F_n}\big)\sum_{j=0}^{2^{k-1}}\left(2^{2^{n+1}}\right)^j \end{aligned}$$

Donc $F_n | F_{n+k}-2$.

Ainsi, $\boxed{\forall n \in \mathbb{N},\ \forall k \in \mathbb{N}^*,\ F_n \text{ divise } F_{n+k}-2.}$

Autre approche :
$$\begin{aligned} F_n \equiv 0\ [F_n] \quad &\Rightarrow \quad F_n - 1 \equiv 2^{2^n} \equiv -1\ [F_n] \\ &\Rightarrow \quad \left(2^{2^n}\right)^{2^k} \equiv 2^{2^n 2^k} \equiv 2^{2^{n+k}} \equiv (-1)^{2^k} \equiv 1\ [F_n] \\ &\Rightarrow \quad F_{n+k}-1 \equiv 1\ [F_n] \quad \Rightarrow \quad F_{n+k}-2 \equiv 0\ [F_n] \end{aligned}$$

b) Soit $(m,n) \in \mathbb{N}^2$. Supposons, sans perte de généralité, que $m < n$.

D'après **??**, avec $k = n-m \in \mathbb{N}^*$, F_m divise $F_n - 2$. Donc il existe $q \in \mathbb{N}$ tel que :

$$F_m - 2 = qF_n \quad \Leftrightarrow \quad F_{n+k} - qF_n = 2$$

Ainsi $F_n \wedge F_m$ divise 2. Or F_n est impair, donc 2 ne divise aucun nombre de Fermat.

Ainsi, $F_n \wedge F_m = 1$.

Ainsi, $\boxed{\forall (m,n) \in \mathbb{N}^2,\ m \neq n \quad \Rightarrow \quad F_m \text{ et } F_n \text{ sont premiers entre eux.}}$

3. Recherche sur la forme de diviseurs premiers de F_n :
a) Soit k vérifiant $(\mathcal{E})$. La division euclidienne de k par k_0 donne l'existence de $q, r \in \mathbb{N}$ tel que :

$$k = qk_0 + r \text{ et } r \in [\![0, k_0 - 1]\!]$$

Il vient :

$$\begin{aligned} a^k \equiv 1\ [p] \quad &\Leftrightarrow \quad a^{qk_0+r} \equiv 1\ [p] \quad \Leftrightarrow \quad \left(a^{k_0}\right)^q a^r \equiv 1\ [p] \\ &\Leftrightarrow \quad 1^q a^r \equiv 1\ [p] \quad \Leftrightarrow \quad a^r \equiv 1\ [p] \end{aligned}$$

Par définition de k_0, comme r vérifie $(\mathcal{E})$ et $r < k_0$, alors $r = 0$ et donc k est un multiple de k_0.
Ainsi, $\boxed{\text{tout entier } k \text{ vérifiant } (\mathcal{E}) \text{ est un multiple de } k_0.}$
b) Comme p est un diviseur premier de F_n. Alors

$$F_n \equiv 0\ [p] \quad \Leftrightarrow \quad 2^{2^n} \equiv -1\ [p] \quad \Rightarrow \quad 2^{2^{n+1}} \equiv 1\ [p]$$

Soit m le plus petit entier (non nul) tel que $2^m \equiv 1\ [p]$.
D'après 3a), m divise 2^{n+1}.
Montrons par l'absurde que m ne divise pas 2^n :

Supposons $m = 2^j$ avec $j \leq n$ alors

$$2^m \equiv 1\ [p] \quad \Rightarrow \quad 2^{2^n} = (2^m)^{2^{n-j}} \equiv 1^{2^{n-j}} \equiv 1\ [p]$$

ce qui contredit que $p | F_n$ autrement dit $2^{2^n} \equiv -1\ [p]$.

Donc, $m = 2^{n+1}$.
Ainsi, $\boxed{2^{n+1} \text{ est le plus petit entier } m \text{ vérifiant } 2^m \equiv 1\ [p].}$
c) Comme p est un diviseur F_n qui est impair alors $2 \wedge p = 1$.
Ainsi, $\boxed{\text{le petit théorème de Fermat donne que } 2^{p-1} \equiv 1\ [p].}$
d) D'après 3a), 2^{n+1} divise $p - 1$.
Ainsi, $\boxed{\text{il existe } j \in \mathbb{N} \text{ tel que } p = 2^{n+1} \times j + 1.}$
e) Raisonnons par l'absurde, supposons que j soit une puissance de 2.
Alors il existe $m \in \mathbb{N}$ tel que $p = 2^m + 1$.
D'après 1c), comme p est premier, alors m est un puissance de 2 et donc p est un nombre de Fermat.
Or, d'après 2b), les nombres de Fermat sont premiers entre eux. Comme p est supposé un diviseur strict de F_n, il y a une contradiction.
Ainsi, $\boxed{\text{l'entier } j \text{ possède un diviseur impair supérieur à 3.}}$
f) Les diviseurs premiers de $F_5 = 2^{2^5} + 1$ doivent être cherché sous la forme :

$$2^6 \times j + 1 \text{ avec } j \in \{3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, \dots\}$$

j n'étant pas une puissance de 2. Il suffit de 6 tentatives pour trouver $p = 641 = 2^6 \times 10 + 1$ diviseur de F_5 ce qui met fin à la conjecture de Fermat !
4. Quelques propriétés des nombres de Fermat :
a) Soit $n \in \mathbb{N}$, $F_{n+1} = 2^{2^{n+1}} + 1 = 2^{(2^n \times 2)} + 1 = \left(2^{2^n}\right)^2 + 1 = \left(2^{2^n} + 1 - 1\right)^2 + 1 = (F_n - 1)^2 + 1$
Ainsi, $\boxed{\forall n \in \mathbb{N},\ F_{n+1} = (F_n - 1)^2 + 1}$
b) Soit $n \in \mathbb{N}$, d'après ce qui précède,

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

Ainsi, $\boxed{\forall n \in \mathbb{N},\ F_{n+1} - 2 = F_n(F_n - 2)}$

c) Procédons par récurrence sur $n \in \mathbb{N}$:

- Initialisation : $F_1 - 2 = 5 - 2 = 3 = F_0$
- Hérédité : Soit $n \geq 1$, on suppose que $F_n - 2 = \prod_{k=0}^{n-1} F_k$. D'après la question précédente :

$$F_{n+1} - 2 = F_n(F_n - 2) = F_n \times \prod_{k=0}^{n-1} F_k = \prod_{k=0}^{n} F_k$$

Ainsi, $\boxed{\forall n \in \mathbb{N}^*,\ F_n - 2 = \prod_{k=0}^{n-1} F_k.}$

Remarque : Sachant que les nombre de Fermat sont impairs, nous pourrions établir que les nombres de Fermat sont premiers en eux à partir de ce dernier résultat.

d) Procédons par récurrence sur $n \geq 2$:

- Initialisation : $F_2 = 17 \equiv 7\ [10]$
- Hérédité : Soit $n \geq 2$. On suppose que $F_n \equiv 7\ [10]$.

$$\begin{aligned} F_n \equiv 7\ [10] \quad &\Rightarrow \quad F_n - 1 \equiv 6\ [10] \quad \Rightarrow \quad (F_n - 1)^2 \equiv 36 \equiv 6\ [10] \\ &\Rightarrow \quad (F_n - 1)^2 + 1 \equiv 7\ [10] \quad \Rightarrow \quad F_{n+1} \equiv 7\ [10] \text{ d'après } \textbf{??} \end{aligned}$$

Ainsi, $\boxed{\text{pour } n \geq 2 \text{ le chiffre des unités de } F_n \text{ est } 7.}$

e) Pour $n \in \mathbb{N}$,

$$\begin{aligned} 2^{F_n} - 2 \ &\equiv 2^{2^{2^n}+1} - 1 \equiv 2\left(2^{2^{2^n}} - 1\right) \equiv 2^{2^{2^n}} - 1\ [F_n] \text{ car } 2 \wedge F_n = 1 \text{ corollaire de Gauss} \\ &\equiv 2^{2^n 2^{2^n - n}} - 1 \equiv \left(2^{2^n}\right)^{2^{2^n - n}} - 1 \equiv (-1)^{2^{2^n - n}} - 1\ [F_n] \\ &\equiv 1 - 1 \equiv 0\ [F_n] \text{ car } n < 2^n \end{aligned}$$

Ainsi, par transitivité de la divisibilité, $\boxed{\forall n \in \mathbb{N},\ F_n \text{ divise } 2^{F_n} - 2.}$