Corrigé du Devoir à la Maison n°4

Nombres de Fermat

Partie A. Définition

1. (a) Première méthode. On utilise la congruence.
Tout d'abord $a+1 \equiv 0\ [a+1]$ donne $a \equiv -1\ [a+1]$.
En conséquence $a^u \equiv (-1)^u\ [a+1]$ et comme u est impair alors $(-1)^u = -1$, donc $a^u \equiv -1\ [a+1]$ puis $a^u + 1 \equiv 0\ [a+1]$.
Ceci montre que $a+1$ divise a^u+1.
Seconde méthode. Comme u est impair alors $(-1)^u = -1$.
On utilise la formule pour $a^n - b^n$. Elle donne :

$$a^u + 1 = a^u - (-1)^u = (a-(-1))\sum_{k=0}^{u-1} a^{u-1-k}(-1)^k = (a+1)\sum_{k=0}^{u-1} a^k(-1)^{u-1-k}$$

Comme la somme est une somme d'entiers alors elle est entière, donc $a+1$ divise a^u+1.

(b) Supposons que a^u+1 est premier.
D'après la question précédente $a+1$ est un diviseur de a^u+1, or un nombre premier n'admet pour diviseurs que 1 et lui-même, donc $a+1=1$ ou $a+1=a^u+1$.
Si $a+1=1$ alors $a=0$, mais a est supposé strictement positif donc ce cas n'est pas possible.
Donc $a+1=a^u+1$, puis $a^u=a$. En appliquant le logarithme népérien on en déduit $u\ln a = \ln a$, et comme a est strictement supérieur à 1 alors $\ln a$ est non-nul donc $u=1$.
On a démontré que si a^u+1 est premier alors $u=1$.

2. (a) Soit m la valuation 2-adique de n. Alors m est un entier et 2^m est la plus grande puissance de 2 qui divise m, ce qui signifie que n s'écrit $2^n u$ avec u non multiple de 2, donc u est impair.

(b) Supposons que 2^m+1 est premier.
Comme $2^m+1 = 2^{2^n u}+1$ alors $(2^{2^n})^u+1$ est premier.
D'après la question (1b), pour $a>1$ et u impair, si a^u+1 est premier alors $u=1$.
On pose $a=2^{2^n}$. Comme $n \geqslant 0$ alors $2^n \geqslant 1$ donc $2^{2^n} \geqslant 2$.
Ainsi $2^m+1 = a^u+1$ est premier, avec $a>1$ et u impair, donc $u=1$.
On en déduit que $m=2^n$, *i.e.,* m est une puissance de 2.

Partie B. Non-primalité de F_5

1. Comme $2^4 + 5^4 \equiv 0\ [5^4 + 2^4]$ alors $2^4 \equiv -5^4\ [5^4 + 2^4]$ puis par implications :

$$\begin{aligned} 2^4 \equiv -5^4\ \left[5^4 + 2^4\right] \quad &\Longrightarrow \quad 2^4 \times 2^{28} \equiv -5^4 \times 2^{28}\ \left[5^4 + 2^4\right] \\ &\Longleftrightarrow \quad 2^{32} \equiv -(5 \times 2^7)^4\ \left[5^4 + 2^4\right] \end{aligned}$$

   On a bien obtenu : $2^{32} \equiv -(5 \times 2^7)^4\ [5^4 + 2^4]$

2. On calcule $5^4 + 2^4 = 625 + 16 = 641$ et $2^7 \times 5 = 2^6 \times 10 = 640$.
   D'après la question précédente :

$$2^{32} \equiv -640^4\ [641]$$

   Or $640 \equiv -1\ [641]$ donc :

$$2^{32} \equiv -(-1)^4 = -1\ [641]$$

   Comme $F^5 = 2^{2^5} + 1$ alors :

$$F_5 = 2^{32} + 1 \equiv 0\ [641]$$

   Ceci montre que F_5 est divisible par 641, qui est strictement compris entre 1 et F_5, donc il n'est pas premier.

Partie C. Les F_n sont premiers entre eux.

1. On démontre par récurrence que la propriété $\mathcal{P}_n$: $F_n = 2 + \prod_{k=0}^{n-1} F_k$ est vraie pour tout $n \in \mathbb{N}$.
   Initialisation. Par définition $F_0 = 2^{2^0} + 1 = 3$. D'autre part un produit vide est égal à 1, donc $2 + \prod_{k=0}^{-1} F_k = 3$, et ainsi la propriété $\mathcal{P}_0$ est vraie.
   Hérédité. Soit $n \in \mathbb{N}$. Supposons que la propriété $\mathcal{P}_n$ est vraie et démontrons qu'alors la propriété $\mathcal{P}_{n+1}$ est vraie.
   Comme $\mathcal{P}_n$ est vraie alors $\prod_{k=0}^{n-1} F_k = F_n - 2$, donc :

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

   Par définition des nombres de Fermat :

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

   Ceci montre que la propriété $\mathcal{P}_{n+1}$ est vraie.
   La propriété $\mathcal{P}_n$ est donc héréditaire.
   Conclusion. La propriété $\mathcal{P}_0$ est vraie, et pour tout $n \in \mathbb{N}$ la propriété $\mathcal{P}_n$ implique la propriété $\mathcal{P}_{n+1}$. Par récurrence, la propriété $\mathcal{P}_n$ est vraie pour tout $n \in \mathbb{N}$.

2. Comme $0 \leqslant m < n$ alors la propriété que nous venons de démontrer s'écrit :

$$F_n = F_m \times \prod_{\substack{0 \leqslant k \leqslant n-1 \\ k \neq m}} F_k + 2$$

On pose :

$$q = \prod_{\substack{0 \leqslant k \leqslant n-1 \\ k \neq m}} F_k$$

Alors q est entier et :

$$F_n = qF_m + 2 \qquad \text{avec} \qquad 0 \leqslant 2 < F_m$$

Cette dernière condition est vérifiée car les nombres de Fermat sont strictement supérieurs à 2 : $m \geqslant 0$ donc $2^m \geqslant 1$ puis $2^{(2^m)} \geqslant 2$ et enfin $F_m \geqslant 3$.

Ceci montre que q et 2 sont respectivement le quotient et le reste de la division euclidienne de F_n par F_m.

3. Par propriété, pour tout couple d'entier (a, b), si r est le quotient de la division euclidienne de a par b alors $a \wedge b = b \wedge r$.

Comme $m \geqslant 0$ alors $2^m \geqslant 1$ puis $2^{(2^m)}$ est pair, ainsi $F_m = 2^{(2^m)} + 1$ est impair. La division euclidienne de F_m par 2 admet $r = 1$ pour reste.

On en déduit :

$$F_n \wedge F_m = F_m \wedge 2 = 2 \wedge 1 = 1$$

Il s'agit en fait de l'algorithme d'Euclide :

$$\begin{array}{rcl} F_n &=& q \times F_m + 2 \\ F_m &=& q' \times 2 + 1 \qquad \text{avec } q \in \mathbb{Z} \\ 2 &=& 2 \times 1 + 0 \end{array}$$

Le dernier reste non-nul est 1, donc le PGCD de F_n et F_m est 1.

Ainsi F_n et F_m sont premiers entre eux.

Ceci est valable dès que m et n sont deux entiers distincts, car on peut supposer que $m < n$ quitte à les inverser.

Ainsi deux nombres de Fermat distincts sont premiers entre eux.

Partie D. Facteurs premiers de F_n

1. D'après le petit théorème de Fermat : $2^p \equiv 2 \ [p]$

Ceci signifie que $2^p - 2 \equiv 0 \ [p]$ donc p divise $2^p - 2$.

On a supposé que p est impair, donc il est premier avec 2. Or $2^p - 2 = 2(2^{p-1} - 1)$.

Ainsi p divise $2 \times (2^{p-1} - 1)$ et p est premier avec 2 donc d'après le lemme de Gauss, p divise $2^{p-1} - 1$.

En conséquence $2^{p-1} - 1 \equiv 0 \ [p]$ puis $2^{p-1} \equiv 1 \ [p]$.

Comme p est un nombre premier impair alors $p > 2$ donc $p - 1 > 0$.

Comme $M = \left\{ k \in \mathbb{N}^* \mid 2^k \equiv 1 \ [p] \right\}$ alors $p - 1$ appartient à M.

2. L'ensemble M est une partie de $\mathbb{N}$, non-vide puisqu'elle contient $p-1$. Elle admet donc un minimum.

3. Comme M est une partie de $\mathbb{N}^*$ alors m est non-nul. On peut donc appliquer la division euclidienne de k par m. Il existe deux entiers q et r tels que :

$$k = qm + r \qquad \text{avec} \qquad 0 \leqslant r < m$$

Comme k et m appartiennent à M alors 2^k et 2^m sont congrus à 1 modulo p. Or :

$$2^k = 2^{mq+r} = (2^m)^q \times 2^r$$

Modulo p ceci donne :

$$1 \equiv 1^q \times 2^r \ \ [p]$$

Ainsi $2^r \equiv 1 \ \ [p]$.

Si r est non-nul alors ceci implique que $r \in M$.

Mais comme $0 \leqslant r < m$ et m est le minimum de M, alors r n'appartient pas à M. Cette contradiction montre que $r = 0$.

Comme $r = 0$ alors $k = qm$, et donc m divise k.

4. On suppose que p divise $F_n = 2^{2^n} + 1$.

Ceci donne $\quad 2^{2^n} + 1 \equiv 0 \ \ [p] \quad$ puis $\quad 2^{2^n} \equiv -1 \ \ [p]$.

Comme p est impair alors -1 n'est pas congru à 1 modulo p. En effet ceci reviendrait à $2 \equiv 0 \ \ [p]$ alors que p ne divise pas 2.

Donc 2^{2^n} n'est pas congru à 1 modulo p et ainsi 2^n n'appartient pas à M.

Par contre $\quad 2^{2^n} \equiv -1 \ \ [p] \quad$ donne $\quad \left(2^{2^n}\right)^2 \equiv (-1)^2 \ \ [p] \quad$ donc $\quad 2^{2^{n+1}} \equiv 1 \ \ [p]$, et ainsi 2^{n+1} appartient à M.

Comme 2^{n+1} appartient à M alors d'après la question (3) m divise 2^{n+1}.

Les seuls diviseurs de 2^{n+1} sont les 2^j pour $j = 0, \ldots, n+1$.

Si $j < n+1$ alors $j \leqslant n$, donc 2^n est un multiple de 2^j, donc de m, ce qui montrerai que $2^n \in M$, alors que ceci est faux d'après ce qui précède.

Donc $j = n+1$, et $m = 2^{n+1}$.

5. D'après la question (1) on sait que $p-1$ appartient à M.

D'après la question (3) on en déduit que m divise $p-1$.

D'après la question précédente on sait que $m = 2^{n+1}$, donc 2^{n+1} divise $p-1$.

Ceci montre que $\quad p - 1 \equiv 0 \ \ [2^{n+1}] \quad$ donc $\quad p \equiv 1 \ \ [2^{n+1}]$.

Il existe donc un entier ℓ tel que $p = 1 + 2^{n+1}\ell$.

Les diviseurs premiers de F_n sont donc bien de la forme $p = 2^{n+1}\ell + 1$ où ℓ est un entier.

Par exemple pour $n = 5$ et $\ell = 10$ on obtient $p = 2^6 \times 10 + 1 = 641$, c'est le diviseur de F_5 que nous avons obtenu dans la partie B.