Groupes finis et arithmétique basique

1 Énoncé

Si p, q sont deux entiers relatifs, on note $p \wedge q$ le pgcd de p et q et $p \vee q$ le ppcm de p et q.

– I – Les nombres de Fermat

On appelle nombre de Fermat tout entier de la forme :

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

où n est un entier naturel.

On vérifie que F_n est premier pour $n = 0, 1, 2, 3, 4$:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537.$$

Fermat pensait que tous les F_n sont premiers, mais Euler prouva que F_5 est non premier. On a vérifié ensuite que les F_n pour n allant de 6 à 11 ne sont pas premiers. On conjecture qu'il n'y a qu'un nombre fini d'entiers de Fermat premiers.

1. Montrer que, pour tout $n \geq 2$, le chiffre des unités de F_n est égal à 7.
2. Montrer que pour tout $n \in \mathbb{N}$, F_n et F_{n+1} sont premiers entre eux.
3. Montrer que pour $n \neq m$ dans $\mathbb{N}$, F_n et F_m sont premiers entre eux.
4. Montrer que pour $n \neq m$ dans $\mathbb{N}$ et p dans $\mathbb{N}^*$, F_n^p et F_m^p sont premiers entre eux.
5. Montrer que :
$$\forall n \geq 0,\ F_{n+1} = \prod_{k=0}^{n} F_k + 2.$$
6. Soient $r \geq 1$ et $a \geq 2$ deux entiers.
   (a) Montrer que si $a^r + 1$ est premier, alors a est pair et il existe un entier $n \geq 0$ tel que $r = 2^n$.
   (b) Montrer que pour tout entier pair $a \geq 2$, les entiers $u_n = a^{2^n} + 1$ sont deux à deux premiers entre eux.
7. Montrer que, pour tout $n \geq 0$, F_n divise $2^{F_n} - 2$.
   À l'époque de Fermat, on pensait que si un entier $m \geq 2$ est tel que m divise $2^m - 2$, alors m est premier, ce qui est faux comme le montre la valeur de $m = 341 = 11 \times 31$, mais c'est quand même vrai pour plusieurs valeurs de m. On peut imaginer que partant de ce résultat Fermat pensait que les F_n sont tous premiers.
8. Montrer que, pour $n \geq 2$, F_n ne peut pas s'écrire comme somme de deux nombres premiers.

– II – Un théorème de Lagrange

Les groupes sont notés multiplicativement et on note 1 l'élément neutre.

Si G est un groupe, pour tout a dans G, on note $\langle a\rangle = \left\{a^k \mid k \in \mathbb{Z}\right\}$ le sous groupe de G engendré par a.

Si $\langle a\rangle$ est infini, on dit alors que a est d'ordre infini dans G, sinon on dit que a est d'ordre fini dans G et l'ordre de a est $\theta(a) = \operatorname{card}(\langle a\rangle)$.

Tous les groupes considérés dans cette section sont finis avec au moins deux éléments.

Pour tout entier naturel $n \geq 2$, on note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ l'anneau des classes résiduelles modulo n, $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles de cet anneau et $\varphi(n)$ le nombre d'éléments de $\mathbb{Z}_n^\times$ (indicateur d'Euler). On pose $\varphi(1) = 1$.

Si k est un entier relatif, on note $\overline{k} = k + n\mathbb{Z}$ la classe de k dans $\mathbb{Z}_n$.

1. Soient G un groupe fini et H un sous-groupe. On rappelle que la relation $g \backsim h$ si et seulement si $g^{-1}h \in H$ est une relation d'équivalence sur G. L'ensemble quotient $\dfrac{G}{H}$ est l'ensemble des classes à gauche selon H :
$$gH = \{gh \mid h \in H\},$$
où g décrit G. Le cardinal de $\dfrac{G}{H}$ est noté $[G : H]$ et appelé l'indice de H dans G.
   (a) Montrer que pour tout $g \in G$ la classe à gauche gH est de cardinal égal à celui de H.
   (b) Montrer que l'ordre de H divise celui de G (théorème de Lagrange).

2. Quelques applications du théorème de Lagrange.
   (a) Montrer qu'un groupe fini de cardinal premier est cyclique.
   (b) Petit théorème de Fermat. Soit p un nombre premier. Montrer que pour tout entier relatif k, $k^p - k$ est divisible par p.
   (c) Théorème d'Euler.
      i. Montrer que pour tout entier naturel $n \geq 2$, $\varphi(n)$ est le nombre de générateurs du groupe cyclique $(\mathbb{Z}_n, +)$.
      ii. Montrer que pour tout entier naturel $n \geq 2$, $\varphi(n)$ est le nombre d'entiers compris entre 1 et n premiers avec n.
      iii. Montrer que pour tout entier relatif k premier avec n, $k^{\varphi(n)} - 1$ est divisible par n.
   (d) Sous-groupes d'un groupe cyclique. On se donne un entier $n \geq 2$.
      i. Montrer que les sous-groupes de $(\mathbb{Z}_n, +)$ sont cycliques d'ordre un diviseur de n.
      ii. Montrer que pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d de $(\mathbb{Z}_n, +)$.
   (e) Montrer que si x, y sont deux éléments d'un groupe fini G d'ordres respectifs p et q premiers entre eux tels que $xy = yx$, alors xy est d'ordre pq. Si p et q ne sont pas premiers entre eux, xy est-il d'ordre $p \vee q$?
   (f) Soient G un groupe commutatif et x, y deux éléments de G d'ordres respectifs p et q. Montrer qu'il existe dans G un élément d'ordre $p \vee q$.
   (g) Soient G un groupe commutatif fini et μ le plus grand des ordres des éléments de G (l'exposant de G). Montrer que pour tout $x \in G$ on a $x^\mu = 1$.
   (h) Montrer que si $\mathbb{K}$ est un corps commutatif, alors tout sous-groupe fini de $\mathbb{K}^*$ est cyclique. En particulier, $\mathbb{Z}_p^*$ est cyclique pour p premier.
   (i) Diviseurs premiers des nombres de Fermat. On désigne par p un diviseur premier d'un nombre de Fermat F_n et on suppose que $p \neq F_n$.

i. Montrer que $p \geq 3$.

ii. Montrer que $\overline{2}$ est d'ordre 2^{n+1} dans le groupe multiplicatif $\mathbb{Z}_p^*$.

iii. Montrer que p congru à 1 modulo 2^{n+1}.

iv. Montrer que $p = 2^{n+1}q + 1$, où q est un entier qui admet un diviseur premier impair.

Pour $F_5 = 4\,294\,967\,297$, s'il n'est pas premier ses diviseurs premiers sont de la forme $p = 2^6 q + 1 = 64q + 1$ où les valeurs possibles de q sont $3, 5, 6, 7, 9, 10, \cdots$ En essayant successivement ces valeurs, on aboutit à :

$$\frac{F_5}{641} = \frac{4\,294\,967\,297}{641} = 6700\,417$$

et F_5 n'est pas premier.

v. Montrer que, pour $n \geq 1$, F_n est premier avec n.

– III – Infinitude de l'ensemble P des nombres premiers

On se propose ici de donner plusieurs démonstration du théorème d'Euclide sur l'infinitude de l'ensemble $\mathcal{P}$ des nombres premiers.

Preuve 1 Rappeler la démonstration d'Euclide de l'infinitude de l'ensemble $\mathcal{P}$ des nombres premiers.

Preuve 2 Montrer que pour tout entier naturel n, on peut trouver un nombre premier p plus grand que n. Conclure.

Preuve 3 On note :

$$\mathcal{P}_1 = \{p \in \mathcal{P} \mid \exists n \in \mathbb{N}\ ;\ p = 4n + 3\}$$
$$\mathcal{P}_2 = \{p \in \mathcal{P} \mid \exists n \in \mathbb{N}\ ;\ p = 6n + 5\}$$

(a) Montrer que $\mathcal{P}_1$ est infini. Conclure.

(b) Montrer que $\mathcal{P}_2$ est infini. Conclure.

De manière plus générale on peut montrer que si a et b sont deux entiers premiers entre eux alors il existe une infinité de nombres premiers de la forme $an + b$ (théorème de Dirichlet).

Preuve 4

(a) Montrer que si on dispose d'une suite $(u_n)_{n\in\mathbb{N}}$ strictement croissante d'entiers naturels différents de 0 et 1 et deux à deux premiers entre eux, on peut alors en déduire que $\mathcal{P}$ infini.

(b) En utilisant les nombres de Fermat, montrer que $\mathcal{P}$ infini.

(c) Soient a, b deux entiers naturels non nuls premiers entre eux avec $b > a$. On définit la suite $(u_n)_{n\in\mathbb{N}}$ par :

$$\begin{cases} u_0 = b \\ \forall n \geq 1,\ u_n - a = u_{n-1}\left(u_{n-1} - a\right) \end{cases}$$

On a vu en première partie, que la suite $(F_n)_{n\in\mathbb{N}}$ des nombres de Fermat vérifie la relation de récurrence :

$$\begin{cases} F_0 = 3 \\ \forall n \geq 1,\ F_n - 2 = F_{n-1}\left(F_{n-1} - 2\right) \end{cases}$$

L'idée est donc de généraliser.

i. Montrer que $(u_n)_{n\in\mathbb{N}}$ est une suite strictement croissante d'entiers naturels différents de 0 et 1.

ii. Montrer que pour tous $m > n \geq 0$, on a :

$$u_m \equiv a \mod u_n$$

iii. Montrer que, pour tout $n \geq 0$, u_n est premier avec a.

iv. Montrer que les u_n sont deux à deux premiers entre eux. Conclure.

(d) Soit a un entiers naturel impair supérieur ou égal à 3. On définit la suite $(u_n)_{n\in\mathbb{N}}$ par :

$$\begin{cases} u_0 = a \\ \forall n \geq 1,\ u_n = u_{n-1}^2 - 2 \end{cases}$$

i. Montrer que $(u_n)_{n\in\mathbb{N}}$ est une suite strictement croissante d'entiers naturels impairs.

ii. Montrer que, pour tout entier naturel n, on a :

$$\begin{cases} u_{n+1} \equiv -2 \mod u_n \\ \forall m \geq n+2,\ u_m \equiv 2 \mod u_n \end{cases}$$

iii. Montrer que les u_n sont deux à deux premiers entre eux. Conclure.

Preuve 5

(a) Soit p un nombre premier impair. On se propose de montrer que $-\overline{1}$ est un carré dans $\mathbb{Z}_p$ si, et seulement si, p est congru à 1 modulo 4.

i. Montrer que si $p \equiv 3 \mod 4$, alors $-\overline{1}$ n'est pas un carré dans $\mathbb{Z}_p$ (ce qui revient à dire que l'équation $x^2 + \overline{1} = 0$ n'a pas de solutions dans $\mathbb{Z}_p$).

ii. Montrer que si $p \equiv 1 \mod 4$, alors l'équation $x^2 + \overline{1} = 0$ a deux solutions dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ qui sont $\overline{-r!}$ et $\overline{r!}$ où $r = \dfrac{p-1}{2}$ ($-\overline{1}$ est alors un carré dans $\mathbb{Z}_p$).

(b) Montrer que l'ensemble :

$$\mathcal{P}_3 = \{p \in \mathcal{P} \mid \exists n \in \mathbb{N}^* \ ;\ p = 4n+1\}$$

est infini et conclure.

Pour les preuves **6.** à **11.** on suppose que $\mathcal{P}$ est fini et on note $p_1 = 2 < \cdots, < p_r$ tous ses éléments (p_r et donc le plus grand nombre premier).
Pour tout réel x, on note $[x]$ sa partie entière.

Preuve 6 Pour tout entier k compris entre 1 et r, on note $n = \prod\limits_{k=1}^{r} p_k = p_k q_k$. En utilisant les diviseurs premiers de $S = \sum\limits_{k=1}^{r} q_k$, montrer qu'on aboutit à une contradiction et conclure.

Preuve 7 Montrer que si p est un diviseur premier de $m = 2^{p_r} - 1$, alors $\overline{2}$ est d'ordre p_r dans le groupe multiplicatif $\mathbb{Z}_p^*$ et conclure.

Preuve 8 Soit n un entier naturel non nul.

(a) Soit m un entier compris entre 1 et 2^n. Montrer que si $m = \prod\limits_{k=1}^{r} p_k^{\alpha_k}$ est la décomposition en facteurs premiers de m, on a alors $\alpha_k \leq n$ pour tout k compris entre 1 et r.

(b) En déduire que $2^n \leq (n+1)^r$ et conclure.

Preuve 9 Soit n un entier naturel non nul.

(a) Soit m un entier compris entre 1 et p_r^n. Montrer que si $m = \prod_{k=1}^{r} p_k^{\alpha_k}$ est la décomposition en facteurs premiers de m, on a alors $\alpha_k \leq \left[n \dfrac{\ln(p_r)}{\ln(2)} \right]$ pour tout k compris entre 1 et r.

(b) En déduire que $p_r^n \leq n^r \left(\dfrac{\ln(p_r)}{\ln(2)} + 1 \right)^r$ et conclure.

Preuve 10

(a) Soient x un réel strictement supérieur à 1, n un entier naturel compris entre 1 et x et $n = \prod_{k=1}^{r} p_k^{\alpha_k}$ la décomposition en facteurs premiers de n où les α_k sont des entiers positifs ou nuls. Montrer que pour tout k compris entre 1 et r, on a :

$$\alpha_k \leq \left[\frac{\ln(x)}{\ln(2)} \right].$$

(b) En déduire que pour tout réel $x > 1$, on a :

$$x < \left(\frac{\ln(2x)}{\ln(2)} \right)^r + 1$$

et conclure.

Preuve 11

(a) Montrer, le plus simplement possible, que la série $\sum \dfrac{1}{n^2}$ est convergente de somme $S \in]0, 2[$.

(b) Pour $n > \prod_{k=1}^{r} p_k$, on partitionne l'ensemble $E = \{1, 2, \cdots, n\}$ en distinguant les entiers compris entre 1 et n qui sont sans facteurs carrés (i. e. de la forme $\prod_{k=1}^{r} p_k^{\varepsilon_k}$ où $(\varepsilon_1, \cdots, \varepsilon_r) \in \{0,1\}^r$) de ceux qui sont divisibles par le carré d'un nombre premier, soit $E = E_1 \cup E_2$, où :

$$E_1 = \left\{ m \in E \mid m = \prod_{k=1}^{r} p_k^{\varepsilon_k} \text{ où } (\varepsilon_1, \cdots, \varepsilon_r) \in \{0,1\}^r \right\}$$
$$E_2 = \left\{ m \in E \mid \exists p_k \in \mathcal{P} \text{ tel que } p_k^2 \text{ divise } m \right\}$$

i. Montrer que $\operatorname{card}(E_1) \leq 2^r$.

ii. Montrer que, pour k compris entre 1 et r, il y a au plus $\left[\dfrac{n}{p_k^2} \right]$ entiers m dans E divisibles par p_k^2 et en déduire que :

$$\operatorname{card}(E_2) \leq n(S-1).$$

iii. Conclure.

– IV – Quelques applications

1. On note $2 = p_1 < p_2 < \cdots < p_n < \cdots$ la suite infini des nombres premiers et on se propose de montrer que $\sum\limits_{n=1}^{+\infty} \dfrac{1}{p_n} = +\infty$. Pour ce faire, on raisonne par l'absurde en supposant que la série à termes positifs $\sum \dfrac{1}{p_n}$ est convergente. Pour tout $n \geq 1$, on note :

$$R_n = \sum_{k=n+1}^{+\infty} \frac{1}{p_k}$$

le reste d'ordre n de cette série.

   (a) Montrer qu'il existe un entier $r \geq 1$ tel que :

   $$\forall n \geq r,\ 0 < R_n < \frac{1}{2}.$$

   Un tel entier r étant fixé, on note $\mathcal{P}_1 = \{p_1, \cdots, p_r\}$ et $\mathcal{P}_2 = \{p_k \mid k \geq r+1\}$.

   (b) Pour tout entier naturel non nul N, on partitionne l'ensemble $E = \{1, 2, \cdots, N\}$ en distinguant les entiers compris entre 1 et N qui ont tous leurs diviseurs premiers dans $\mathcal{P}_1$ de ceux qui ont au moins un diviseur dans $\mathcal{P}_2$, soit $E = E_1 \cup E_2$, où :

   $$E_1 = \left\{ n \in E \mid n = \prod_{k=1}^{r} p_k^{\alpha_k} \text{ où } (\alpha_1, \cdots, \alpha_r) \in \mathbb{N}^r \right\}$$
   $$E_2 = \{n \in E \mid \exists p_k \in \mathcal{P}_2 \text{ qui divise } n\}$$

      i. En écrivant tout entier n dans E_1 sous la forme $n = pq^2$ où p, q sont deux entiers naturels non nul, l'entier p étant égal à 1 ou sans facteurs carrés (i. e. $p = \prod\limits_{k=1}^{r} p_k^{\varepsilon_k}$ où $(\varepsilon_1, \cdots, \varepsilon_r) \in \{0,1\}^r$), montrer que :

      $$N_1 = \operatorname{card}(E_1) \leq 2^r \left[\sqrt{N}\right]$$

      ($[\cdot]$ désigne toujours la partie entière).

      ii. Montrer que pour tout p_k dans $\mathcal{P}_2$, il y a au plus $\left[\dfrac{N}{p_k}\right]$ entiers n dans E divisibles par p_k et en déduire que :

      $$N_2 = \operatorname{card}(E_2) < \frac{N}{2}.$$

      iii. Conclure.

2. La divergence de la série $\sum\limits_{n=1}^{+\infty} \dfrac{1}{p_n}$ peut aussi se montrer de façon plus classique comme suit en utilisant la suite $(u_n)_{n \geq 1}$ définie par :

$$\forall n \geq 1,\ u_n = \frac{1}{\prod\limits_{k=1}^{n} \left(1 - \frac{1}{p_k}\right)}.$$

   (a) Montrer que, pour tout $n \geq 1$, on a :

   $$u_n = \sum_{k \in E_n} \frac{1}{k}$$

   où E_n est l'ensemble des les entiers naturels non nuls qui ont tous leurs diviseurs premiers dans $\mathcal{P}_n = \{p_1, \cdots, p_n\}$.

(b) En déduire que, pour tout $n \geq 1$, on a :

$$u_n \geq \sum_{k=1}^{p_n} \frac{1}{k}.$$

(c) En déduire que la série $\sum \ln\left(1 - \frac{1}{p_n}\right)$ est divergente et conclure.

3. Quelle est la nature de la série $\sum \frac{1}{p_n^\alpha}$ où α est un réel ?

4. Quelle est le rayon de convergence de la série entière $\sum \frac{z^{p_n}}{p_n}$.

   Si Q est un polynôme à coefficients entiers relatifs de degré supérieur ou égal à 1 et p un nombre premier, on dit que p divise Q s'il existe un entier relatif a tel que p divise $Q(a)$.

5. On se propose de montrer dans cette question le théorème de Schur suivant : *tout polynôme non constant à coefficients entiers relatifs admet une infinité de diviseurs premier.*

   (a) Montrer que tout polynôme à coefficients entiers relatifs non constant admet des diviseurs premiers.

   (b) Montrer que tout polynôme Q à coefficients entiers relatifs non constant tel que $Q(0) = 0$ admet une infinité des diviseurs premiers.

   (c) Soit :

   $$Q(X) = \sum_{k=0}^{n} a_k X^k$$

   un polynôme à coefficients entiers relatifs de degré $n \geq 1$ non nul en 0.
   On suppose que l'ensemble des diviseurs premiers de Q est fini et on le note :

   $$\mathcal{P}_Q = \{p_1, \cdots, p_r\}.$$

   On note aussi $m = \prod_{k=1}^{r} p_k$.

   i. Montrer qu'il existe un polynôme $R(X) = \sum_{k=1}^{n} b_k X^k$ de degré n dans $\mathbb{Z}[X]$ tel que $Q(a_0 m X) = a_0 (1 + R(X))$, chaque coefficient b_k, pour k compris entre 1 et r, étant divisible par m.

   ii. En utilisant les diviseurs premiers de $1+R$, montrer qu'on aboutit à une contradiction et conclure.

6. En utilisant le polynôme $Q(X) = 4X^2 + 1$, retrouver le fait qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

7. Soit q un nombre premier impair.
   En utilisant le polynôme $Q(X) = 1 + X + \cdots + X^{q-1}$, montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo q.

   Pour tout entier naturel $n \in \mathbb{N}^*$, on note $\omega_n = \exp\left(\frac{2i\pi}{n}\right)$ et on définit le polynôme cyclotomique Φ_n par :

   $$\Phi_n(X) = \prod_{\substack{k=1 \\ k \wedge n = 1}}^{n} \left(X - \omega_n^k\right)$$

   (les ω_n^k pour k premier avec n et $1 \leq k \leq n$ sont les racines primitives n-ème de l'unité).
   Pour tout entier naturel $n \in \mathbb{N}^*$, on note $\mathcal{D}_n$ l'ensemble des diviseurs de n dans $\mathbb{N}^*$.
   On admet les résultats suivants :

– pour tout $n \in \mathbb{N}^*$ on a :

$$X^n - 1 = \prod_{d \in \mathcal{D}_n} \Phi_d(X)$$

– pour tout $n \in \mathbb{N}^*$, Φ_n est un polynôme à coefficients entiers.

On se propose de montrer dans les deux questions qui suivent, le résultat suivant : *si $n \geq 2$ est un entier naturel et p un nombre premier ne divisant pas n, alors p divise Φ_n si, et seulement si, p est congru à 1 modulo n.*

8. Montrer que si p est un nombre premier congru à 1 modulo n, alors p divise Φ_n.
9. On se donne un entier $n \geq 2$ et un nombre premier p qui divise Φ_n.
   (a) Montrer que pour tout polynôme Q à coefficients entiers et tout entier a, on a :

   $$Q(a+p) \equiv Q(a) \mod p.$$

   (b) Montrer qu'il existe un entier naturel a tel que l'ordre d de $\overline{a}$ dans le groupe multiplicatif $\mathbb{Z}_p^*$ soit un diviseur de n.
   (c) Montrer que si $d = n$, alors p est congru à 1 modulo n.
   (d) On suppose que $d < n$.
      i. Montrer que $a^n - 1$ est divisible par p^2.
      ii. Montrer que $(a+p)^n - 1$ est divisible par p^2.
      iii. Montrer que $na^{n-1}p$ est divisible par p^2 et que si on suppose de plus p est premier avec n, on aboutit alors à une contradiction.

   (e) Conclure.
10. Déduire de ce qui précède, le cas particulier suivant du théorème de Dirichlet : pour tout entier $n \geq 1$, il existe une infinité de nombres premiers de la forme $1 + kn$ où $k \in \mathbb{N}^*$.

2 Corrigé

– I – Les nombres de Fermat

1. Pour $n = 2$, on a $F_2 = 17$. En supposant que, pour $n \geq 2$, F_n est congru à 7 modulo 10 (équivalent à dire que 7 est le chiffre des unités de F_n), on a :

$$\begin{aligned} F_{n+1} &= 2^{2^{n+1}} + 1 = \left(2^{2n}\right)^2 + 1 = (F_n - 1)^2 + 1 \\ &\equiv 6^2 + 1 = 37 \equiv 7 \mod 10. \end{aligned}$$

2.

Solution 1 On a :

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

avec $2 < F_n$, c'est donc la division euclidienne de F_{n+1} par F_n avec 2 pour reste et :

$$F_n \wedge F_{n+1} = F_n \wedge 2 = 1$$

puisque F_n est impair.

Solution 2 On peut aussi remarquer que :

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

soit :

$$q_nF_n=F_{n+1}-2$$

c'est encore la division euclidienne de F_{n+1} par F_n avec 2 pour reste et :

$$F_n\wedge F_{n+1}=F_n\wedge 2=1.$$

Solution 3 Ou remarquer que :

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

donc le pgcd δ de F_n et F_{n+1} est impair et divise 2^p avec $p\geq 1$, il vaut donc 1.

Solution 4 Notons $x=2^{2n}$. Si p premier divise F_n, p est impair comme F_n et on a $\overline{F_n}=\overline{0}$ dans $\mathbb{Z}_p$, soit $\overline{x}=-1$ et $\overline{F_{n+1}}=(\overline{x})^2+\overline{1}=\overline{2}\neq\overline{0}$ dans $\mathbb{Z}_p$ puisque $p\neq 2$, ce qui signifie que p ne divise pas F_{n+1}. Donc F_n et F_{n+1} sont premiers entre eux.

3. Comme n et m jouent des rôles symétriques, on peut supposer que $m=n+p>n$ avec $p\geq 1$.

Solution 1 On a :

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

et en utilisant la formule du binôme, il vient :

$$F_m-1=q_{n,m}F_n+1$$

soit :

$$F_m=q_{n,m}F_n+2$$

avec $2<F_n$, c'est-à-dire la division euclidienne de F_m par F_n avec 2 pour reste et :

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

Solution 2 Si p premier divise F_n, p est impair comme F_n et on a $\overline{F_n}=\overline{0}$ dans $\mathbb{Z}_p$, soit $\overline{x}=-1$ et $\overline{F_m}=(\overline{x})^{2^{m-n}}+\overline{1}=\overline{2}\neq\overline{0}$ dans $\mathbb{Z}_p$ puisque $p\neq 2$, ce qui signifie que p ne divise pas F_m. Donc F_n et F_m sont premiers entre eux.

4. Avec $F_n^p\wedge F_m^p=(F_n\wedge F_m)^p$ pour tout $p\geq 1$, on déduit que pour $n\neq m$, F_n^p et F_m^p sont premiers entre eux.
   On peut aussi dire que F_n et F_m sont sans facteurs premiers communs puisque premiers entre eux et il en est de même de F_n^p et F_m^p.
5. On procède par récurrence sur $n\geq 0$.
   Pour $n=0$, on a :

$$F_1=2^2+1=5=F_0+2.$$

En supposant le résultat acquis pour $n-1\geq 0$, on a :

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

On a donc $F_{n+1}=q_nF_n+2$ et on retrouve ainsi le fait que F_{n+1} et F_n sont premiers entre eux.

6.

(a) Supposons que a soit impair, on a donc $a \geq 3$ et $a^r + 1$ est un nombre pair supérieur ou égal à 4, il ne peut être premier. L'entier a est donc nécessairement pair si $a^r + 1$ est premier.
En utilisant la décomposition en facteurs premiers, on a $r = 2^n (2q+1)$ où n et q sont deux entiers naturels et :

$$\begin{aligned} a^r + 1 &= \left(a^{2^n}\right)^{2q+1} + 1 = b^{2q+1} + 1 \\ &= (b+1)\left(b^{2q} - b^{2q-1} + b^{2q-2} - \cdots + 1\right) \\ &= (b+1) \sum_{k=0}^{2q} (-1)^k b^{2q-k} = (b+1) S \end{aligned}$$

avec $b + 1 = a^{2^n} + 1 \geq 3$ puisque $a \geq 2$ et :

$$S = \frac{a^r + 1}{b+1} = \frac{b^{2q+1} + 1}{b+1} = \frac{b^{2q} b + 1}{b+1} > \frac{b+1}{b+1} = 1$$

si $q \geq 1$, soit $S \geq 2$ puisque c'est un entier et l'entier $a^r + 1$ n'est pas premier dans ce cas. On a donc $q = 0$ et $r = 2^n$.

(b) On procède comme pour les nombres de Fermat. Supposons que $m = n + p$ avec $p \geq 1$. On a alors :

$$u_m - 1 = a^{2^{n+p}} = \left(a^{2^n}\right)^{2^p} = (u_n - 1)^{2^p}$$

et en utilisant la formule du binôme, il vient :

$$u_m - 1 = q_{n,m} u_n + 1$$

soit :

$$u_m = q_{n,m} u_n + 2$$

(division euclidienne) et le pgcd δ de u_n et u_m est impair (puisque u_n est impair) et divise 2, il vaut donc 1.

7. $F_n = 2^{2^n} + 1$ divise $\left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = 2^{2^{n+1}} - 1$ et comme $2^n \geq n+1$, $2^{2^{n+1}} - 1$ divise $2^{2^{2^n}} - 1$ qui divise $2\left(2^{2^{2^n}} - 1\right) = 2^{2^{2^n}+1} - 2 = 2^{F_n} - 2$, donc F_n divise $2^{F_n} - 2$.

8. Si $F_n = p + q$ avec p et q premiers, on a nécessairement $p = 2$ et $q \geq 3$ puisque F_n est impair et :

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

avec $F_{n-1} \geq 5$, $F_{n-1} - 2 \geq 3$ pour $n \geq 2$, ce qui est incompatible avec q premier.

– II – Un théorème de Lagrange

1.

(a) Pour g fixé dans G, la translation $\tau_g : h \mapsto gh$ est une application bijective de G dans G et sa restriction à H réalise une bijection de H sur gH. Il en résulte que gH et H ont même cardinal.

(b) L'ensemble des classes à gauche suivant H réalise une partition de G et elles sont en nombre fini de même cardinal égal à celui de H, il en résulte que :

$$\operatorname{card}(G) = [G : H] \operatorname{card}(H)$$

et $\operatorname{card}(H)$ divise $\operatorname{card}(G)$.

2.

(a) Soient G un groupe de cardinal premier $p \geq 2$ et $g \in G \setminus \{1\}$. Le sous-groupe $\langle g \rangle$ de G engendré par g n'est pas réduit à l'élément neutre et de cardinal $q \geq 2$ qui doit diviser p premier, on a donc $q = p$ et $\langle g \rangle = G$, c'est-à-dire que G est cyclique engendré par g. L'application $\overline{k} \mapsto g^k$ réalise alors un isomorphisme du groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}, + \right)$ sur $(G, \cdot)$.

(b) Si p est premier alors $\mathbb{Z}_p$ est un corps (conséquence du théorème de Bézout) et $\mathbb{Z}_p^*$ est un groupe multiplicatif à $p-1$ éléments. Tout élément $\overline{k}$ dans $\mathbb{Z}_p^*$ a alors un ordre qui divise $p-1$, ce qui entraîne que pour tout entier k non multiple de p, k^{p-1} est congru à 1 modulo p, ce qui est encore équivalent à dire que $k^{p-1} - 1$ est divisible par p et donc que $k^p - k$ est divisible par p. Si k est multiple de p, il en est de même de $k^p - k$.

(c)

i. Dire que $\overline{k}$ est inversible dans $\mathbb{Z}_n$ équivaut à dire qu'il existe $\overline{u} \in \mathbb{Z}_n$ tel que $\overline{k}\overline{u} = \overline{1}$ encore équivalent à dire qu'il existe $u \in \mathbb{Z}$ tel que $u\overline{k} = \overline{1}$, soit à dire que $\overline{1}$ est dans le groupe engendré par $\overline{k}$ et donc que ce groupe est $\mathbb{Z}_n$. Donc $\overline{k} \in \mathbb{Z}_n^\times$ si et seulement si $\overline{k}$ est générateur du groupe additif $\mathbb{Z}_n$. Il en résulte que $\varphi(n)$ est le nombre de générateurs du groupe cyclique $(\mathbb{Z}_n, +)$.

ii. Dire que $\overline{k}$ est inversible dans $\mathbb{Z}_n$ équivaut à dire qu'il existe $\overline{u} \in \mathbb{Z}_n$ tel que $\overline{k}\overline{u} = \overline{1}$ encore équivalent à dire qu'il existe deux entiers relatifs u et v tels que $ku + nv = 1$ équivalent à dire que k et n sont premiers entre eux (théorème de Bézout). En considérant que chaque classe modulo n a un unique représentant compris entre 1 et n, on déduit que $\varphi(n)$ est le nombre d'entiers compris entre 1 et n premiers avec n.

On peut remarquer que $\frac{\varphi(n)}{n}$ est la probabilité pour qu'un entier choisi de manière équiprobable entre 1 et n soit premier avec n (n est le nombre de cas possibles et $\varphi(n)$ le nombre de cas favorables).

iii. Si k est premier avec n, alors $\overline{k}$ appartient à $\mathbb{Z}_n^\times$ qui est d'ordre $\varphi(n)$ et $\overline{k}^{\varphi(n)} = \overline{1}$, c'est-à-dire que $k^{\varphi(n)} \equiv 1 \pmod{n}$. Pour p premier, on a $\varphi(p) = p-1$ et on retrouve le théorème de Fermat.

(d)

i. Soit H un sous-groupe de $(\mathbb{Z}_n, +)$. Son ordre d divise n et $m = \frac{n}{d}$ est un entier.

Pour tout $\overline{k} \in H$, on a $d\overline{k} = \overline{0}$ (l'ordre de $\overline{k}$ divise d), soit $dk = qn$ et $k = qm$, soit $\overline{k} = q\overline{m} \in \langle \overline{m} \rangle$. On a donc $H \subset \langle \overline{m} \rangle$ et $d = \text{card}(H) \leq \theta(\overline{m})$. Mais $d\overline{m} = \overline{n} = \overline{0}$, donc d est multiple de $\theta(\overline{m})$ et $d \geq \theta(\overline{m})$. On a donc $d = \theta(\overline{m})$ et $H = \langle \overline{m} \rangle$ est cyclique. Au passage, on a montré que $\langle \overline{m} \rangle$ est l'unique sous-groupe d'ordre d de $(\mathbb{Z}_n, +)$.

ii. Réciproquement soit d un diviseur de n. Le groupe $H = \langle \overline{m} \rangle = \left\langle \overline{\frac{n}{d}} \right\rangle$ est cyclique d'ordre $\theta(\overline{m})$. De $d\overline{m} = \overline{0}$, on déduit que d est multiple de $\theta(\overline{m})$ et $d \geq \theta(\overline{m})$. De $\theta(\overline{m})\,\overline{m} = \overline{0}$, on déduit que $\theta(\overline{m})\, m = qn = qdm$ et $\theta(\overline{m}) = qd \geq d$. Donc $d = \theta(\overline{m})$ et $H = \langle \overline{m} \rangle$ est l'unique sous-groupe d'ordre d de $(\mathbb{Z}_n, +)$.

(e) On a $(xy)^{pq} = (x^p)^q (y^q)^p = 1$ puisque x et y commutent. L'ordre $r = \theta(xy)$ de xy est donc un diviseur de pq et $\theta(xy) \leq pq$. À ce stade le fait que p et q soient premiers entre eux n'intervient pas.

L'égalité $(xy)^r = x^r y^r = 1$ entraîne $y^r = (x^r)^{-1} \in \langle x \rangle \cap \langle y \rangle = H$. Le groupe H étant contenu dans les groupes $\langle x \rangle$ et $\langle y \rangle$ a un ordre qui divise p et q et ces entiers étant premiers entre eux, on a nécessairement $H = \{1\}$. On a donc $y^r = x^r = 1$ et r est un

multiple de p et q, donc de pq puisque p et q sont premiers entre eux. On peut donc conclure à l'égalité $\theta(xy) = pq$.
On peut aussi écrire que $(xy)^r = 1$ entraîne $(xy)^{rp} = y^{rp} = 1$, donc q divise rp et q divise r puisque p et q sont premiers entre eux. Les éléments x et y jouant des rôles symétriques, on a de même p qui divise r. On conclut alors comme précédemment.
Si p et q ne sont pas premiers entre eux, on peut seulement dire que l'ordre de xy divise pq. Ce n'est pas nécessairement le ppcm des ordres de x et y. En prenant par exemple, x d'ordre $p \geq 2$ dans G et $y = x^{-1}$ qui est également d'ordre p, on $xy = 1$ d'ordre $1 \neq \text{ppcm}(p, p) = p$.

(f) Si p et q sont premiers entre eux, on vient de voir que $z = xy$ est d'ordre $pq = p \vee q$. L'idée est de se ramener à ce cas de figure.
On peut écrire les décompositions en facteurs premiers :

$$p = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\alpha_i},\ q = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{i=k+1}^{r} p_i^{\beta_i}$$

où les facteurs premiers p_i ont été regroupés de sorte que $\alpha_i > \beta_i$ pour $1 \leq i \leq k$ et $\alpha_i \leq \beta_i$ pour $k+1 \leq i \leq r$, les exposants α_i, β_i étant positifs ou nuls (si l'une des conditions $\alpha_i > \beta_i$ ou $\alpha_i \leq \beta_i$ n'est jamais vérifiée, alors le produit correspondant vaut 1). On a alors :

$$p \vee q = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\beta_i} = rs,$$

où $r = \prod\limits_{i=1}^{k} p_i^{\alpha_i}$ et $s = \prod\limits_{i=k+1}^{r} p_i^{\beta_i}$ sont premiers entre eux et $p = ru$, $q = sv$. Les éléments $x' = x^u$ et $y' = y^v$ sont alors d'ordres respectifs r et s et la question précédente nous dit que $z = x^u y^v$ est d'ordre $rs = p \vee q$.

(g) Si μ est le plus grand des ordres des éléments de G (il existe puisque G est fini), il existe x_0 d'ordre μ dans G.
Pour tout $x \in G$ d'ordre p, on peut trouver $y \in G$ d'ordre $p \vee \mu \geq \mu$ et nécessairement $p \vee \mu = \mu$ puisque μ est le plus grand des ordres. Donc p divise μ et $x^\mu = 1$.

(h) Soit G un sous groupe d'ordre n de $\mathbb{K}^*$. Il existe dans G (commutatif) un élément x d'ordre $\mu \leq n$ égal au plus grand des ordres des éléments de G. L'ordre de tout élément de G divisant μ, on déduit que tout $y \in G$ est racine du polynôme $P(X) = X^\mu - 1$, ce qui donne n racines de P dans $\mathbb{K}$, mais sur un corps commutatif un polynôme de degré μ a au plus μ racines[1], on a donc $n \leq \mu$, soit $\mu = n$ et G ayant un élément d'ordre n est cyclique.

(i)

i. Comme F_n est impair, on a nécessairement $p \geq 3$.

ii. On a $F_n = 2^{2^n} + 1 = pq_n$ avec p premier et $q_n \geq 2$ entier naturel ($p \neq F_n$), donc $\overline{F_n} = \overline{0}$ dans $\mathbb{Z}_p$, soit $\overline{2}^{2^n} = -\overline{1}$ dans $\mathbb{Z}_p^*$ et $\overline{2}^{2^{n+1}} = \left(\overline{2}^{2^n}\right)^2 = \left(-\overline{1}\right)^2 = \overline{1}$ et l'ordre de $\overline{2}$ dans le groupe multiplicatif $\mathbb{Z}_p^*$ est un diviseur de 2^{n+1}, donc de la forme 2^k avec $1 \leq k \leq n+1$, mais avec $\overline{2}^{2^n} = -\overline{1} \neq \overline{1}$ (puisque $p \neq 2$) on déduit que cet ordre est exactement 2^{n+1}.

iii. 2^{n+1} est donc un diviseur de $p - 1 = \text{card}\left(\mathbb{Z}_p^*\right)$, ce qui peut se traduire par $p - 1$ congru à 0 modulo 2^{n+1} ou encore p congru à 1 modulo 2^{n+1}.

[1]Ce résultat est faux sur un corps non commutatif, voir par exemple le corps des quaternions.

iv. Dire que p est congru à 1 modulo 2^{n+1} signifie qu'il existe un entier $q \geq 1$ tel que $p = 2^{n+1}q + 1$. Si q n'admet aucun diviseur premier impair, il est de la forme $q = 2^m$ avec $m \geq 0$ et $p = 2^{n+1+m} + 1$ est premier, ce qui impose que $n+1+m = 2^r$ (question 6a), c'est-à-dire que $p = 2^{2^r} + 1$ est un nombre de Fermat et $p = F_n$ puisque deux nombres de Fermat distincts sont premiers entre eux, en contradiction avec $p \neq F_n$. Donc q admet un diviseur premier impair.

v. Les diviseurs premiers de F_n étant de la forme $p = 2^{n+1}q + 1$ avec $q \geq 1$, ils sont tous strictement plus grands que n, donc n est premier avec F_n puisqu'ils ne peuvent avoir de diviseurs premiers en commun.

– III – Infinitude de l'ensemble P des nombres premiers

Preuve 1 On sait déjà que $\mathcal{P}$ est non vide (il contient 2). Supposons que $\mathcal{P}$ soit fini avec :

$$\mathcal{P} = \{p_1, \cdots, p_r\}.$$

L'entier $n = p_1 \cdots p_r + 1$ est supérieur ou égal à 2, il admet donc un diviseur premier $p_k \in \mathcal{P}$. L'entier p_k divise alors $n = p_1 \cdots p_r + 1$ et $p_1 \cdots p_r$, il divise donc la différence qui est égale à 1, ce qui est impossible. En conclusion $\mathcal{P}$ est infini.

Preuve 2 Pour tout $n \in \mathbb{N}$, l'entier $m = n! + 1 \geq 2$ admet un diviseur premier p_n. Si $p_n < n$ alors p_n est un diviseur de $n!$, donc de $1 = m - n!$, ce qui est impossible. On a donc ainsi une suite strictement croissante $(p_n)_{n\in\mathbb{N}}$ de nombres premiers, ce qui implique que $\mathcal{P}$ est infini.

Preuve 3

(a) On remarque qu'un nombre premier différent de 2 est nécessairement impair et son reste dans la division euclidienne par 4 ne peut être que 1 ou 3.
Supposons que $\mathcal{P}_1$ soit fini et notons $3 = p_1 < p_2 < \cdots < p_r$ tous ses éléments. L'entier :

$$m = 4p_1 \cdots p_r - 1 = 4(p_1 \cdots p_r - 1) + 3$$

qui est de la forme $4n + 3$ avec $n \geq 2$ n'est pas premier puisque strictement supérieur à tous les p_k pour k compris entre 1 et r ($m > 4p_k - 1 > p_k$ puisque $p_k \geq 3$). Comme m est impair, ses diviseurs premiers sont de la forme $4k + 1$ avec $k \in \mathbb{N}^*$ ou $4k + 3$ avec $k \in \mathbb{N}$ et ils ne peuvent pas être tous de la forme $4k+1$, sans quoi m serait aussi de cette forme, donc congru à 1 modulo 4, ce qui contredit le fait qu'il est congru à 3 (ou à -1) modulo 4. L'entier m a donc un diviseur p_k dans $\mathcal{P}_1$ et comme p_k divise $p_1 \cdots p_r$, il va aussi diviser -1, ce qui est impossible avec p_k premier. L'ensemble $\mathcal{P}_1$ est donc infini.
De $\mathcal{P}_1 \subset \mathcal{P}$, on déduit que $\mathcal{P}$ est infini.

(b) Supposons que $\mathcal{P}_2$ soit fini et notons $5 = p_1 < p_2 < \cdots < p_r$ tous ses éléments. L'entier :

$$m = 6p_1 \cdots p_r - 1 = 6(p_1 \cdots p_r - 1) + 5$$

qui est de la forme $6n + 5$ avec $n \geq 2$ n'est pas premier puisque strictement supérieur à tous les p_k pour k compris entre 1 et r ($m > 6p_k - 1 > p_k$ puisque $p_k \geq 5$). Comme m est impair non multiple de 3 (il est congru à 5 modulo 3) ses diviseurs premiers sont de la forme $6k + 1$ avec $k \in \mathbb{N}^*$ ou $6k + 5$ avec $k \in \mathbb{N}$ et ils ne peuvent pas être tous de la forme $6k + 1$, sans quoi m serait aussi de cette forme, donc congru à 1 modulo 6, ce qui contredit le fait qu'il est congru à 5 modulo 6. L'entier m a donc un diviseur p_k dans $\mathcal{P}_2$ et comme p_k divise $p_1 \cdots p_r$, il va aussi diviser -1, ce qui est impossible avec p_k premier. L'ensemble $\mathcal{P}_2$ est donc infini.
De $\mathcal{P}_2 \subset \mathcal{P}$, on déduit que $\mathcal{P}$ est infini.

Preuve 4

(a) En désignant, pour tout entier naturel n, par p_n un diviseur premier de u_n, on a $p_n \neq p_m$ pour tous $n \neq m$ puisque u_n et u_m sont premiers entre eux et donc ne peuvent avoir un diviseur premier en commun. La suite $(p_n)_{n\in\mathbb{N}}$ nous fournit donc une infinité de nombres premiers.

(b) Résulte du fait que la suite $(F_n)_{n\in\mathbb{N}}$ des nombres de Fermat est strictement croissante dans $\mathbb{N} \setminus \{0,1\}$ et que deux nombres de Fermat distincts sont premiers entre eux.

(c)

i. On vérifie facilement par récurrence que $(u_n)_{n\in\mathbb{N}}$ est une suite d'entiers naturels et que $u_n > a \geq 1$ pour tout $n \in \mathbb{N}$. En effet, $u_0 = b > a$ avec $b \in \mathbb{N}$ et supposant le résultat acquis au rang $n-1$, on a $u_n = a + u_{n-1}(u_{n-1} - a) \in \mathbb{N}$ et :

$$u_n - a = u_{n-1}(u_{n-1} - a) > 0.$$

On en déduit que pour tout $n \geq 1$, on a :

$$u_n - u_{n-1} = a + u_{n-1}(u_{n-1} - a - 1) \geq a > 0$$

($u_{n-1} > a$ dans $\mathbb{N}$ équivaut à $u_{n-1} \geq a+1$), c'est-à-dire que $(u_n)_{n\in\mathbb{N}}$ est strictement croissante à valeurs dans $\mathbb{N} \setminus \{0,1\}$.

ii. On procède par récurrence sur $m > n$, à $n \geq 0$ fixé.
Pour $m = n+1$, on a :

$$u_{n+1} - a = u_n(u_n - a) \equiv 0 \mod u_n$$

et supposant le résultat acquis au rang $m-1 > n$, on a :

$$u_m - a = u_{m-1}(u_{m-1} - a) \equiv 0 \mod u_n.$$

On a donc :

$$u_m = q_{n,m}u_n + a$$

avec $0 \leq a < u_n$, c'est-à-dire que a est le reste dans la division euclidienne de a par u_n.

iii. Pour $n = 0$, on a $u_0 = b$ qui est premier avec a par hypothèse.
Supposons le résultat acquis au rang $n-1 \geq 1$ et soit $\delta = u_n \wedge a$. Si $\delta \geq 2$, il admet alors un diviseur premier p qui divise u_n et a. Avec $u_n - a = u_{n-1}(u_{n-1} - a)$, on déduit que p divise $u_{n-1}(u_{n-1} - a)$ et en conséquence divise u_{n-1} ou $u_{n-1} - a$. Mais p ne peut diviser u_{n-1} puisqu'il divise a et a est premier avec u_{n-1}, donc p divise $u_{n-1} - a$ et aussi $u_{n-1} = (u_{n-1} - a) + a$, ce qui est impossible. On a donc $\delta = 1$.

iv. On procède comme pour les nombres de Fermat. À partir de la division euclidienne $u_m = q_{n,m}u_n + a$ (pour $m > n \geq 0$) on déduit que :

$$u_m \wedge u_n = u_n \wedge a = 1.$$

Il en résulte que $\mathcal{P}$ est infini.

(d)

i. On vérifie facilement par récurrence que $(u_n)_{n\in\mathbb{N}}$ est une suite d'entiers naturels impairs tous différents de 1. En effet, $u_0 = a$ est impair avec $a \geq 3$ et supposant le résultat acquis au rang $n-1$, $u_n = u_{n-1}^2 - 2$ est un entier impair et :

$$u_n \geq 9 - 2 \geq 3.$$

On en déduit que pour tout $n \geq 1$, on a :

$$u_n - u_{n-1} = u_{n-1}(u_{n-1} - 1) - 2 \geq 6 - 2 > 0$$

c'est-à-dire que $(u_n)_{n\in\mathbb{N}}$ est strictement croissante.

ii. Par définition de u_n, on a $u_{n+1} \equiv -2 \mod u_n$ et :

$$u_{n+2} = u_{n+1}^2 - 2 \equiv (-2)^2 - 2 = 2 \mod u_n.$$

En supposant que $u_m \equiv 2 \mod u_n$ pour $m \geq n+2$, on a :

$$u_{m+1} = u_m^2 - 2 \equiv (-2)^2 - 2 = 2 \mod u_n.$$

On a donc ainsi vérifié par récurrence, que pour tout $m \geq n+2$, on a $u_m \equiv 2 \mod u_n$.

iii. Pour $m > n \geq 0$, on a $u_m = qu_n + r$ avec $r = \pm 2$ ($u_m \equiv \pm 2 \mod u_n$), il en résulte que :

$$u_m \wedge u_n = u_n \wedge (\pm 2) = 1$$

puisque u_n est impair.
On en déduit que $\mathcal{P}$ est infini.

Preuve 5

(a)

i. Dire $p \equiv 3 \bmod 4$ revient à dire qu'il existe un entier $n \geq 0$ tel que $p = 4n+3$. On a alors $r = \dfrac{p-1}{2} = 2n+1$ et si $x \in \mathbb{Z}_p^*$ est tel que $x^2 = -\overline{1}$, il vient $x^{p-1} = x^{2r} = \left(-\overline{1}\right)^{2n+1} = -\overline{1}$, ce qui contredit le théorème de Fermat qui nous dit que $x^{p-1} = \overline{1}$ pour tout $x \in \mathbb{Z}_p^*$ (on a $-\overline{1} \neq \overline{1}$ puisque $p \geq 2$).

ii. Le théorème de Wilson nous dit que $\overline{(p-1)!} = -\overline{1}$ dans $\mathbb{Z}_p^*$ puisque p est premier. Par ailleurs, pour $k = 1, \cdots, r$, on a :

$$r + k \equiv -r + k - 1 \mod p$$

(c'est équivalent à $2r = p - 1 \equiv -1 \mod p$), soit :

$$r + k \equiv -(r - (k-1)) \mod p$$

et :

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot \cdots \cdot r \cdot (r+1) \cdots (r+r) \\ &\equiv r!\,(-1)^r\, r\,(r-1) \cdots 1 = (-1)^r (r!)^2 \mod p\end{aligned}$$

Pour $p \equiv 1 \bmod 4$, on a $p = 4n+1$ avec $n \geq 1$ et $r = \dfrac{p-1}{2} = 2n$, de sorte que $(-1)^r = 1$ et $(p-1)! \equiv (r!)^2 \mod p$, ce qui donne $\overline{r!}^2 = -\overline{1}$ d'après le théorème de Wilson. Donc $-\overline{1}$ est un carré dans $\mathbb{Z}_p^*$. Comme $-\overline{r!}$ est aussi solution de $x^2 + \overline{1} = 0$ avec $-\overline{r!} \neq \overline{r!}$ puisque $p \neq 2$, on a ainsi les deux seules solutions possibles.

(b) Supposons que $\mathcal{P}_3$ soit fini et notons $5 = p_1 < p_2 < \cdots < p_r$ tous ses éléments. L'entier :

$$m = 4p_1^2 \cdots p_r^2 + 1$$

qui est de la forme $4n+1$ avec $n \geq 2$ n'est pas premier puisque strictement supérieur à tous les p_k pour k compris entre 1 et r. Comme m est impair, ses diviseurs premiers sont

de la forme $4k+1$ avec $k \in \mathbb{N}^*$ ou $4k+3$ avec $k \in \mathbb{N}$. Si p est un diviseur premier de m, on a alors $m = a^2+1 = pq$ et $\overline{a}^2 = -\overline{1}$ dans $\mathbb{Z}_p^*$, c'est-à-dire que $-\overline{1}$ est un carré dans $\mathbb{Z}_p^*$ et p est nécessairement de la forme $4k+1$ avec $k \in \mathbb{N}^*$, donc p est l'un des p_k dans $\mathcal{P}_3$ et comme p_k divise $p_1 \cdots p_r$, il va aussi diviser 1 puisqu'il divise m, ce qui est impossible.
L'ensemble $\mathcal{P}_3$ est donc infini.
De $\mathcal{P}_3 \subset \mathcal{P}$, on déduit que $\mathcal{P}$ est infini.

Preuve 6 Si p est un diviseur premier de S, c'est l'un des p_k avec k compris entre 1 et r. En remarquant que pour j compris entre 1 et r différent de k, $q_j = \dfrac{n}{p_j} = \prod\limits_{\substack{i=1 \\ i\neq j}}^{r} p_i$ est divisible par p_k, on déduit que p_k va diviser $q_k = S - \sum\limits_{\substack{j=1 \\ j\neq k}}^{r} q_j$ et pourtant $q_k = \dfrac{n}{p_k} = \prod\limits_{\substack{i=1 \\ i\neq k}}^{r} p_i$ n'est pas divisible par p_k (p_k est premier avec tous les p_j pour $j \neq k$, donc avec leur produit n_k). On aboutit donc ainsi à une contradiction. Il en résulte que $\mathcal{P}$ est infini.
Il est peut être plus simple de travailler dans $\mathbb{Z}_p$ avec $p = p_k$. On a $\overline{S} = \overline{q_k} \neq \overline{0}$ qui est impossible puisque p divise S.

Preuve 7 Si p est un diviseur premier de $m = 2^{p_r} - 1 \geq 2,$, on a alors $m \equiv 0$ modulo p, soit $\overline{2}^{p_r} = \overline{1}$ dans $\mathbb{Z}_p$ et l'ordre de $\overline{2}$ dans le groupe multiplicatif $\mathbb{Z}_p^*$ est un diviseur de p_r et comme p_r est premier, cet ordre est exactement p_r (on a $\overline{2} \neq \overline{1}$ dans $\mathbb{Z}_p$). Donc p_r est un diviseur de $p-1 = \operatorname{card}\left(\mathbb{Z}_p^*\right)$ (théorème de Lagrange) et $p_r < p$, ce qui contredit le fait que p_r et le plus grand nombre premier.
L'ensemble $\mathcal{P}$ est donc infini.

Preuve 8

(a) Tout entier m compris entre 1 et 2^n s'écrit de manière unique $m = \prod\limits_{k=1}^{r} p_k^{\alpha_k}$, où les α_k sont des entiers positifs ou nuls. Pour k compris entre 1 et r, on a $p_k^{\alpha_k} \leq m \leq 2^n$ et nécessairement $\alpha_k \leq n$ (si $\alpha_k > n$, alors $p_k^{\alpha_k} \geq 2^{\alpha_k} > 2^n$).

(b) On peut donc définir l'application :

$$\begin{array}{rccc} \varphi : & E = \{1, 2, \cdots, 2^n\} & \rightarrow & F = \{0, 1, \cdots, n\}^r \\ & m = \prod\limits_{k=1}^{r} p_k^{\alpha_k} & \mapsto & (\alpha_1, \cdots, \alpha_r) \end{array}$$

et cette application est injective, ce qui entraîne :

$$2^n = \operatorname{card}(E) \leq \operatorname{card}(F) = (n+1)^r$$

l'entier naturel non nul n étant quelconque, ce qui est en contradiction avec $\lim\limits_{n\to+\infty} \dfrac{2^n}{(n+1)^r} = +\infty$.
Il en résulte que $\mathcal{P}$ est infini.

Preuve 9

(a) De $p_k^{\alpha_k} \leq m = \prod\limits_{j=1}^{r} p_j^{\alpha_j} \leq p_r^n$, on déduit que $\alpha_k \ln(p_k) \leq n \ln(p_r)$ et :

$$\alpha_k \leq n \frac{\ln(p_r)}{\ln(p_k)} \leq n \frac{\ln(p_r)}{\ln(2)} < \left[n \frac{\ln(p_r)}{\ln(2)} \right] + 1$$

et $0 \leq \alpha_k \leq \left[n \dfrac{\ln(p_r)}{\ln(2)} \right]$.

(b) L'application :

$$\begin{array}{rccc} \varphi : & E = \{1, 2, \cdots, p_r^n\} & \to & F = \left\{0, 1, \cdots, \left[n \dfrac{\ln(p_r)}{\ln(2)}\right]\right\}^r \\ & m = \displaystyle\prod_{k=1}^{r} p_k^{\alpha_k} & \mapsto & (\alpha_1, \cdots, \alpha_r) \end{array}$$

est injective, donc :

$$\begin{aligned} p_r^n = \operatorname{card}(E) \leq \operatorname{card}(F) &= \left(\left[n \frac{\ln(p_r)}{\ln(2)}\right] + 1\right)^r \\ &\leq \left(n \frac{\ln(p_r)}{\ln(2)} + 1\right)^r = n^r \left(\frac{\ln(p_r)}{\ln(2)} + \frac{1}{n}\right)^r \leq n^r \left(\frac{\ln(p_r)}{\ln(2)} + 1\right)^r \end{aligned}$$

ou encore :

$$\frac{p_r^n}{n^r} \leq \left(\frac{\ln(p_r)}{\ln(2)} + 1\right)^r$$

l'entier $n \geq 1$ étant quelconque, ce qui est incompatible avec $\lim\limits_{n \to +\infty} \dfrac{p_r^n}{n^r} = +\infty$.
Il en résulte que $\mathcal{P}$ est infini.

Preuve 10

(a) Soit x un réel strictement supérieur à 1 et n un entier naturel non nul tel que $n \leq x$. On a la décomposition en facteurs premiers $n = \prod\limits_{k=1}^{r} p_k^{\alpha_k}$, où les α_k sont des entiers positifs ou nuls. Pour tout k compris entre 1 et r, on a $p_k^{\alpha_k} \leq n \leq x$ et

$$\alpha_k \leq \frac{\ln(x)}{\ln(p_k)} \leq \frac{\ln(x)}{\ln(p_1)} = \frac{\ln(x)}{\ln(2)} < \left[\frac{\ln(x)}{\ln(2)}\right] + 1$$

soit :

$$\alpha_k \leq \left[\frac{\ln(x)}{\ln(2)}\right]$$

puisque α_k est entier.

(b) Pour $x > 1$, on a $[x] = \operatorname{card}(E_x)$, où :

$$E_x = \{n \in \mathbb{N} \mid 1 \leq n \leq x\}$$

et l'injection :

$$\begin{array}{rccc} \varphi : & E_x & \to & F_x = \left\{0, 1, \cdots, \left[\dfrac{\ln(x)}{\ln(2)}\right]\right\}^r \\ & m = \displaystyle\prod_{k=1}^{r} p_k^{\alpha_k} & \mapsto & (\alpha_1, \cdots, \alpha_r) \end{array}$$

ce qui donne :

$$\begin{aligned} [x] = \operatorname{card}(E_x) \leq \operatorname{card}(F_x) &= \left(\left[\frac{\ln(x)}{\ln(2)}\right] + 1\right)^r \\ &\leq \left(\frac{\ln(x)}{\ln(2)} + 1\right)^r = \left(\frac{\ln(2x)}{\ln(2)}\right)^r \end{aligned}$$

et :

$$x < [x] + 1 \leq \left(\frac{\ln(2x)}{\ln(2)}\right)^r + 1$$

soit :

$$\frac{x}{(\ln(2x))^r} < \frac{1}{(\ln(2))^r} + \frac{1}{(\ln(2x))^r} < 2\frac{1}{(\ln(2))^r}$$

qui est en contradiction avec $\lim\limits_{x\to+\infty} \dfrac{x}{(\ln(2x))^r} = +\infty$.

On en déduit que $\mathcal{P}$ est infini.

Preuve 11

(a) Pour tout $k \geq 2$, on a :

$$\frac{1}{k^2} < \frac{1}{k(k-1)} = \frac{1}{k-1} - \frac{1}{k}$$

et pour $n \geq 2$:

$$S_n = \sum_{k=1}^{n} \frac{1}{k^2} < 1 + \sum_{k=2}^{n} \left(\frac{1}{k-1} - \frac{1}{k}\right) = 2 - \frac{1}{n}$$

avec $\lim\limits_{n\to+\infty} \left(2 - \dfrac{1}{n}\right) = 2$. Il en résulte que la suite croissante $(S_n)_{n\geq1}$ est majorée par 2, elle est donc convergente de limite $S \leq 2$.

En écrivant, pour tout $n \geq 2$, que :

$$\begin{aligned}\frac{1}{n^2} &= \left(\frac{1}{n^2} - \frac{1}{n(n-1)}\right) + \frac{1}{n(n-1)} \\ &= \left(\frac{1}{n-1} - \frac{1}{n}\right) - \frac{1}{n^2(n-1)}\end{aligned}$$

on a :

$$\begin{aligned}S = \sum_{n=1}^{+\infty} \frac{1}{n^2} &= 1 + \sum_{n=2}^{+\infty} \left(\frac{1}{n-1} - \frac{1}{n}\right) - \sum_{n=2}^{+\infty} \frac{1}{n^2(n-1)} \\ &= 2 - \sum_{n=2}^{+\infty} \frac{1}{n^2(n-1)} = 2 - T < 2.\end{aligned}$$

(b)

i. L'application :

$$\begin{array}{rccc} \varphi : & E_1 & \to & F = \{0,1\}^r \\ & m = \prod\limits_{k=1}^{r} p_k^{\varepsilon_k} & \mapsto & (\varepsilon_1, \cdots, \varepsilon_r) \end{array}$$

étant injective, on déduit que :

$$\mathrm{card}(E_1) \leq \mathrm{card}(F) = 2^r.$$

ii. Si $m \in E$ est divisible par p_k^2, on a alors $m = p_k^2 q_k \leq n$ et $q_k = \dfrac{m}{p_k^2} \leq \dfrac{n}{p_{k^2}} < \left[\dfrac{n}{p_k^2}\right] + 1$, soit $q_k \leq \left[\dfrac{n}{p_k^2}\right]$. Il y a donc un maximum de $\left[\dfrac{n}{p_k^2}\right]$ possibilités pour q_k et pour un tel m.

En écrivant que :

$$E_2 = \bigcup_{k=1}^{r} \left\{m \in E \mid m \text{ est divisible par } p_k^2\right\}$$

on déduit que :

$$\operatorname{card}(E_2) \leq \sum_{k=1}^{r} \left[\frac{n}{p_k^2}\right] \leq \sum_{k=1}^{r} \frac{n}{p_k^2} = n \sum_{k=1}^{r} \frac{1}{p_k^2}$$
$$< n \sum_{n=2}^{+\infty} \frac{1}{n^2} = n\,(S-1)\,.$$

iii. On a donc, pour tout entier $n > \prod\limits_{k=1}^{r} p_k$:

$$n = \operatorname{card}(E_1) + \operatorname{card}(E_2) < 2^r + n\,(S-1)$$

soit :

$$0 < (2-S)\,n < 2^r$$

ce qui est impossible pour n assez grand.
Il en résulte que $\mathcal{P}$ est infini.

– IV – Quelques applications

1.

(a) La quantité R_n étant le reste d'ordre n de la série à termes positifs convergente $\sum \frac{1}{p_n}$, on a $\lim\limits_{n\to+\infty} R_n = 0$ et il existe un entier $r \geq 1$ tel que :

$$\forall n \geq r,\ 0 < R_n < \frac{1}{2}.$$

(b) Les ensembles $\mathcal{P}_1$ et $\mathcal{P}_2$ formant une partition de l'ensemble $\mathcal{P}$ des nombres premiers, on peut faire la partition indiquée de E.

i. La décomposition en facteurs premiers de tout entier $n \in E_1$, peut s'écrire sous la forme :

$$n = \prod_{k=1}^{r} p_k^{\alpha_k} = \prod_{k=1}^{r} p_k^{\varepsilon_k} \prod_{k=1}^{r} p_k^{2\beta_k} = pq^2$$

où, pour tout k compris entre 1 et r, on a posé :

$$\varepsilon_k = \begin{cases} 0 \text{ si } \alpha_k \text{ est pair} \\ 1 \text{ si } \alpha_k \text{ est impair} \end{cases}$$

$p = \prod\limits_{k=1}^{r} p_k^{\varepsilon_k}$, $q = \prod\limits_{k=1}^{r} p_k^{\beta_k}$. Le nombre maximum de choix possibles pour p est :

$$\operatorname{card}(\{0,1\}^r) = 2^r$$

et avec $q^2 \leq n \leq N$, on déduit que $q \leq \sqrt{N} < \left[\sqrt{N}\right] + 1$, soit $q \leq \left[\sqrt{N}\right]$ et il y a un maximum de $\left[\sqrt{N}\right]$ choix possibles pour q. On en déduit donc que :

$$N_1 \leq 2^r \left[\sqrt{N}\right].$$

ii. Si $n \in E_2$, il existe un nombre premier $p_k \in \mathcal{P}_2$ qui divise n, c'est-à-dire que $n = p_k q$ et $q = \dfrac{n}{p_k} \leq \dfrac{N}{p_k} < \left[\dfrac{N}{p_k}\right] + 1$, soit $q \leq \left[\dfrac{N}{p_k}\right]$ et il y a un maximum de $\left[\dfrac{N}{p_k}\right]$ choix possibles pour q, donc pour n. Pour p_k grand, on a en fait $\left[\dfrac{N}{p_k}\right] = 0$. On en déduit alors que :

$$N_2 \leq \left[\frac{N}{p_{r+1}}\right] + \left[\frac{N}{p_{r+2}}\right] + \cdots$$

soit :

$$N_2 \leq \sum_{k=r+1}^{+\infty} \left[\frac{N}{p_k}\right] \leq \sum_{k=r+1}^{+\infty} \frac{N}{p_k} = N \sum_{k=r+1}^{+\infty} \frac{1}{p_k} < \frac{N}{2}.$$

iii. On a donc :

$$N = N_1 + N_2 < 2^r \left[\sqrt{N}\right] + \frac{N}{2} \leq 2^r \sqrt{N} + \frac{N}{2}$$

soit :

$$1 \leq 2^r \frac{1}{\sqrt{N}} + \frac{1}{2} \underset{N \to +\infty}{\to} \frac{1}{2}$$

ce qui est impossible. On a donc $\sum\limits_{n=1}^{+\infty} \dfrac{1}{p_n} = +\infty$.

2.

(a) Pour $n \geq 1$, on a :

$$u_n = \prod_{k=1}^{n} \frac{1}{1 - \frac{1}{p_k}} = \prod_{k=1}^{n} \left(\sum_{i=0}^{+\infty} \frac{1}{p_k^i} \right) = \sum_{i_1 \geq 0, i_2 \geq 0, \cdots, i_n \geq 0}^{+\infty} \frac{1}{p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n}}$$
$$= \sum_{k \in E_n} \frac{1}{k}.$$

(b) Résulte du fait que E_n contient $\{1, 2, \cdots, p_n\}$, la série étant à termes positifs.

(c) La suite $\left(\sum\limits_{k=1}^{p_n} \dfrac{1}{k} \right)_{n \geq 1}$ étant extraite de la suite divergente vers l'infini $\left(\sum\limits_{k=1}^{n} \dfrac{1}{k} \right)_{n \geq 1}$, on a $\lim\limits_{n \to +\infty} \sum\limits_{k=1}^{p_n} \dfrac{1}{k} = +\infty$, donc $\lim\limits_{n \to +\infty} u_n = +\infty$ et $\lim\limits_{n \to +\infty} \prod\limits_{k=1}^{n} \left(1 - \dfrac{1}{p_k}\right) = 0$, ce qui entraîne :

$$\lim_{n \to +\infty} \ln \left(\prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right) \right) = \lim_{n \to +\infty} \sum_{k=1}^{n} \ln \left(1 - \frac{1}{p_k}\right) = -\infty$$

La série $\sum \ln \left(1 - \dfrac{1}{p_n}\right)$ est donc divergente. Cette série étant à termes négatifs avec $\ln \left(1 - \dfrac{1}{p_n}\right) \underset{+\infty}{\backsim} -\dfrac{1}{p_n}$, on en déduit la divergence de $\sum \dfrac{1}{p_n}$.
On a aussi la courte démonstration suivante :
Si $\sum\limits_{n=1}^{+\infty} \dfrac{1}{p_n} < +\infty$ il existe alors un entier $r \geq 1$ tel que :

$$R_r = \sum_{n=r+1}^{+\infty} \frac{1}{p_n} < \frac{1}{2}.$$

On note $P = p_1 \cdots p_r$. Pour tout $n \geq 1$, les diviseurs premiers de $1 + nP$ sont dans $\{p_k \mid k \geq r+1\}$ (pour $1 \leq k \leq r$, le nombre premier p_k divisant P ne peut diviser $1+nP$) et on a :

$$1 + nP = p_{r+1}^{m_1} \cdots p_{r+s_n}^{m_{s_n}}$$

avec $s_n \geq 1$, $m_j \geq 0$ pour j compris entre 1 et s_n et $m_{s_n} \geq 1$. On en déduit que pour tout $N \geq 1$, on a :

$$\sum_{n=1}^{N} \frac{1}{1+nq} < \sum_{j=1}^{+\infty} \left(\sum_{n=r+1}^{+\infty} \frac{1}{p_n} \right)^j < \sum_{j=1}^{+\infty} \left(\frac{1}{2} \right)^j$$

en contradiction avec $\sum\limits_{n=1}^{+\infty} \dfrac{1}{1+nq} = +\infty$.

Un théorème de Mertens nous dit que pour tout réel $x \geq 2$, on a :

$$\sum_{p_n \leq x} \frac{1}{p_n} = C + \ln(\ln(x)) + O\left(\frac{1}{\ln(x)} \right)$$

où $C \backsimeq 0.261$.

On a aussi :

$$\sum_{p_n \leq x} \frac{1}{p_n} = \ln(x) + O(1).$$

3. Pour $\alpha \leq 0$, on a $\dfrac{1}{p_n^\alpha} \geq 1$ et la série $\sum \dfrac{1}{p_n^\alpha}$ diverge puisque son terme général ne tend pas vers 0.

   Pour $0 < \alpha \leq 1$, on a $\dfrac{1}{p_n^\alpha} \geq \dfrac{1}{p_n}$ et la série $\sum \dfrac{1}{p_n^\alpha}$ diverge.

   Pour $\alpha > 1$, on a pour tout $n \geq 1$:

$$S_n = \sum_{k=1}^{n} \frac{1}{p_k^\alpha} \leq \sum_{k=1}^{p_n} \frac{1}{k^\alpha} < \sum_{k=1}^{+\infty} \frac{1}{k^\alpha} < +\infty$$

   donc la suite des sommes partielles $(S_n)_{n \geq 1}$ est majorée et la série $\sum \dfrac{1}{p_n^\alpha}$ converge.

4. La série $\sum \dfrac{z^{p_n}}{p_n}$ diverge pour $z = 1$, son rayon de convergence est donc $R \leq 1$.

   Pour $|z| < 1$ et $n \geq 1$, on a $p_n \geq n$ et :

$$\left| \frac{z^{p_n}}{p_n} \right| \leq |z^{p_n}| \leq |z^n|$$

   avec $\sum\limits_{n=1}^{+\infty} |z^n| < +\infty$, donc $\sum\limits_{n=1}^{+\infty} \left| \dfrac{z^{p_n}}{p_n} \right| < +\infty$ et $R \geq 1$. On a donc $R = 1$.

5.

   (a) Soit :

$$Q(X) = \sum_{k=0}^{n} a_k X^k$$

   un polynôme à coefficients entiers relatifs de degré $n \geq 1$.

   Les équations $Q(x) = -1$, $Q(x) = 0$ et $Q(x) = 1$ n'ayant qu'un nombre fini de solutions dans $\mathbb{Z}$, il existe un entier naturel a tel que $|Q(k)| \geq 2$ pour tout entier naturel $k \geq a$. En particulier $Q(a)$ admet des diviseurs premiers.

(b) Si $Q(0)=0$, on a alors $Q(X)=XR(X)$ avec R non nul dans $\mathbb{Z}[X]$ et pour tout nombre premier p, $Q(p)=pR(p)$ est divisible par p. Donc Q admet une infinité de diviseurs premiers.

(c)

i. On a :

$$Q(a_0mX)=\sum_{k=0}^{n}a_ka_0^km^kX^k=a_0\left(1+\sum_{k=1}^{n}a_ka_0^{k-1}m^kX^k\right)$$

les coefficients $b_k=a_ka_0^{k-1}m^k$, pour k compris entre 1 et n étant divisibles par m.

ii. Le polynôme $1+R$ qui est non constant à coefficients entiers admet des diviseurs premiers. Si p est l'un d'eux il existe un entier a tel que p divise $1+R(a)$ et p divise $Q(a_0ma)=a_0(1+R(a))$, c'est-à-dire que p est un diviseur premier de Q, c'est donc l'un des p_k. L'entier p divise alors m et comme m divise tous les coefficients b_k, p va diviser $R(a)$. On est donc dans la situation où p premier divise les entiers $R(a)$ et $1+R(a)$, ce qui entraîne que p divise 1, soit une impossibilité.
En conclusion Q admet une infinité de diviseurs premiers.

6. Le polynôme $Q(X)=4X^2+1$ admettant une infinité de diviseurs premiers, on peut donc trouver une suite strictement croissante $(p_n)_{n\in\mathbb{N}}$ de nombres premiers et une suite $(a_n)_{n\in\mathbb{N}}$ d'entiers relatifs tels que pour tout $n\in\mathbb{N}$, p_n divise $4a_n^2+1$. On a alors $4\overline{a_n}^2=-\overline{1}$ dans $\mathbb{Z}_{p_n}$ et p_n est nécessairement congru à 1 modulo 4, c'est-à-dire que p_n est de la forme $4k+1$.
On dispose ainsi d'une infinité de nombres premiers congrus à 1 modulo 4.

7. Le polynôme $Q(X)=1+X+\cdots+X^{q-1}$ admettant une infinité de diviseurs premiers, on peut donc trouver une suite strictement croissante $(p_n)_{n\in\mathbb{N}}$ de nombres premiers et une suite $(a_n)_{n\in\mathbb{N}}$ d'entiers relatifs tels que pour tout $n\in\mathbb{N}$, p_n divise $Q(a_n)$. Donc, pour $n\in\mathbb{N}$, p_n divise :

$$a_n^q-1=(a_n-1)Q(a_n)$$

et on a $\overline{a_n}^q=\overline{1}$ dans $\mathbb{Z}_{p_n}$, ce qui signifie que $\overline{a_n}$ est d'ordre 1 ou q dans $\mathbb{Z}_{p_n}^*$ puisque q est premier. Dire que $\overline{a_n}$ est d'ordre 1 signifie que $\overline{a_n}=\overline{1}$, donc $\overline{Q(a_n)}=\overline{q}$ avec $\overline{Q(a_n)}=\overline{0}$ puisque p_n divise $Q(a_n)$, l'entier q est donc divisible par p_n et $p_n=q$ puisque ces deux nombres sont premiers. Prenant les p_n tous différents de q (on en a une infinité), on déduit que, pour tout $n\in\mathbb{N}$, $\overline{a_n}$ est d'ordre q dans $\mathbb{Z}_{p_n}^*$ et q divise $p_n-1=\mathrm{card}\left(\mathbb{Z}_{p_n}^*\right)$, ce qui signifie que p_n est congru à 1 modulo q. On dispose ainsi d'une infinité de nombres premiers de la forme $qn+1$.

8. Si p est un nombre premier congru à 1 modulo n, alors n est un diviseur de l'ordre $p-1$ du groupe cyclique $\mathbb{Z}_p^*$ et il existe dans $\mathbb{Z}_p^*$ un élément $\overline{a}$ d'ordre n. De $\overline{0}=\overline{a}^n-\overline{1}=\prod_{d\in\mathcal{D}_n}\overline{\Phi_d(a)}$, on déduit qu'il existe $d\in\mathcal{D}_n$ tel que $\overline{\Phi_d(a)}=\overline{0}$. Si $d<n$, de $\overline{a}^d-\overline{1}=\prod_{\delta\in\mathcal{D}_d}\overline{\Phi_\delta(a)}$, on déduit que $\overline{a}^d=\overline{1}$, ce qui n'est pas compatible avec la définition de l'ordre n de $\overline{a}$. On a donc $d=n$ et $\overline{\Phi_n(a)}=\overline{0}$, ce qui équivaut à dire que p divise $\Phi_n(a)$.

9.

(a) Si Q est un polynôme constant, on alors $Q(a+p)=Q(a)$ pour tout entier a.
Pour tout entier $k\geq 1$, on a :

$$(a+p)^k=a^k+\sum_{j=1}^{k}C_k^ja^{k-j}p^j\equiv a^k \mod p$$

et en conséquence $Q(a+p)\equiv Q(a) \mod p$ pour tout polynôme Q.
Ou plus simplement, on peut écrire dans $\mathbb{Z}_p$:

$$\overline{Q(a+p)}=Q\left(\overline{a+p}\right)=Q(\overline{a})=\overline{Q(a)}$$

(b) Dire que p divise Φ_n équivaut à dire qu'il existe un entier relatif a tel que p divise $\Phi_n(a)$, ce qui revient à dire que $\overline{\Phi_n(a)} = \overline{0}$ dans $\mathbb{Z}_p$. Avec $\overline{a}^n - \overline{1} = \prod_{d \in \mathcal{D}_n} \overline{\Phi_d(a)}$, on déduit que $\overline{a}^n = \overline{1}$ dans $\mathbb{Z}_p$ et l'ordre d de a dans le groupe multiplicatif $\mathbb{Z}_p^*$ est un diviseur de n, soit $d \in \mathcal{D}_n$.

(c) Si $d = n$, alors n est un diviseur de $p-1 = \mathrm{card}\left(\mathbb{Z}_p^*\right)$ (théorème de Lagrange) et $p = 1+kn$ avec $k \in \mathbb{Z}$.

(d)

i. Si $d < n$, de :

$$\overline{0} = \overline{a}^d - \overline{1} = \prod_{\delta \in \mathcal{D}_d} \overline{\Phi_\delta(a)}$$

dans le corps $\mathbb{Z}_p$, on déduit qu'il existe $\delta \in \mathcal{D}_d$ tel que $\overline{\Phi_\delta(a)} = \overline{0}$, ce qui équivaut à dire que $\Phi_\delta(a)$ est divisible par p. L'entier p divise donc $\Phi_n(a)$ et $\Phi_\delta(a)$ où δ est un diviseur de n (δ divise d qui divise n) tel que $\delta < n$, ce qui entraîne que :

$$a^n - 1 = \prod_{d' \in \mathcal{D}_n} \Phi_{d'}(a) = \Phi_\delta(a)\,\Phi_n(a) \prod_{d' \in \mathcal{D}_n - \{\delta, n\}} \Phi_{d'}(a)$$

est divisible par p^2.

ii. On a :

$$(a+p)^n - 1 = \Phi_\delta(a+p)\,\Phi_n(a+p) \prod_{d' \in \mathcal{D}_n - \{\delta, n\}} \Phi_{d'}(a+p)$$

où $\delta \in \mathcal{D}_d$ est tel que $\delta < n$ et $\overline{\Phi_\delta(a)} = \overline{0}$ et comme :

$$\Phi_m(a+p) \equiv \Phi_m(a) \equiv 0 \mod p$$

pour $m = \delta$ et $m = n$ avec $\Phi_m(a)$ divisible par p, on déduit que $(a+p)^n - 1$ est divisible par p^2.

iii. De ce qui précède, on déduit que $(a+p)^n - a^n$ est divisible par p^2 et il existe un entier q tel que :

$$p^2 q = (a+p)^n - a^n = na^{n-1}p + \sum_{k=2}^{n} C_n^k a^{n-k} p^k = na^{n-1}p + p^2 r$$

ce qui entraîne que $na^{n-1}p$ est divisible par p^2 et donc que na^{n-1} est divisible par p. Comme p est premier avec n, on en déduit que a^{n-1} est divisible par p, soit $\overline{a}^{n-1} = \overline{0}$ dans le corps $\mathbb{Z}_p$ et $\overline{a} = \overline{0}$, ce qui contredit $\overline{a}^n = \overline{1}$. On ne peut donc avoir $d < n$ pour p premier avec n.

(e) On a donc, pour p premier avec n, $d = n$ et p est congru à 1 modulo n.

10. Pour $n = 1$, c'est l'infinitude de l'ensemble des nombres premiers.
Comme, pour tout $n \geq 2$, Φ_n admet une infinité de diviseurs premiers, il y en a une infinité qui ne divisent pas n et de tels diviseurs sont nécessairement congrus à 1 modulo p d'après ce qui précède. On déduit donc qu'il existe une infinité de nombres premiers de la forme $1 + kn$ où $k \in \mathbb{N}^*$.