

Corrigés

Corrigé 1

Supposons, sans perte de généralité, que $m > n$. Soit d un diviseur commun à F_n et F_m . Par définition, $F_n = 2^{2^n} + 1 \equiv 0 \pmod{d}$, ce qui implique $2^{2^n} \equiv -1 \pmod{d}$. L'expression de F_m peut être réécrite pour faire apparaître F_n . Comme $m > n$, on a $m = n + k$ pour un certain entier $k \geq 1$.

$$F_m = 2^{2^m} + 1 = 2^{2^{n+k}} + 1 = 2^{2^n \cdot 2^k} + 1 = (2^{2^n})^{2^k} + 1$$

En utilisant la congruence $2^{2^n} \equiv -1 \pmod{d}$, on a :

$$F_m \equiv (-1)^{2^k} + 1 \pmod{d}$$

Puisque $k \geq 1$, 2^k est un nombre pair. Par conséquent, $(-1)^{2^k} = 1$.

$$F_m \equiv 1 + 1 \pmod{d}$$

$$F_m \equiv 2 \pmod{d}$$

Puisque d est un diviseur de F_m , on a aussi $F_m \equiv 0 \pmod{d}$. On en déduit donc que $2 \equiv 0 \pmod{d}$, ce qui signifie que d doit diviser 2. Les seuls diviseurs positifs de 2 sont 1 et 2.

Cependant, les nombres de Fermat $F_n = 2^{2^n} + 1$ sont toujours impairs, car 2^{2^n} est une puissance de 2 paire. Par conséquent, leur seul diviseur commun possible est 1. Donc, F_n et F_m sont premiers entre eux.

Corrigé 2

On cherche les couples d'entiers naturels (m, n) qui sont solutions de l'équation $3^m - 2^n = 1$. On peut immédiatement remarquer deux solutions évidentes :

- Si $m = 1$ et $n = 1$, on a $3^1 - 2^1 = 3 - 2 = 1$.
- Si $m = 2$ et $n = 3$, on a $3^2 - 2^3 = 9 - 8 = 1$.

Nous allons maintenant prouver que ce sont les deux seules solutions en étudiant la parité de l'exposant m .

Cas 1 : m est un entier impair. Soit $m = 2k + 1$ pour un certain $k \in \mathbb{N}$. L'équation s'écrit $3^{2k+1} - 2^n = 1$. Considérons cette équation modulo 4. On sait que $3 \equiv -1 \pmod{4}$. Donc, $3^m \equiv (-1)^m \pmod{4}$. Comme m est impair, $3^m \equiv -1 \pmod{4}$. En substituant dans l'équation, on a $3^m - 1 \equiv 2^n \pmod{4}$, ce qui donne $(-1) - 1 \equiv -2 \equiv 2 \pmod{4}$. Ainsi, $2^n \equiv 2 \pmod{4}$. Cette congruence n'est possible que si $n = 1$, car pour $n \geq 2$, 2^n est un multiple de 4, donc $2^n \equiv 0 \pmod{4}$. Si $n = 1$, l'équation devient $3^m - 2^1 = 1$, ce qui donne $3^m = 3$, d'où $m = 1$. La seule solution dans ce cas est le couple $(1, 1)$.

Cas 2 : m est un entier pair. Soit $m = 2k$ pour un certain $k \in \mathbb{N}^*$. L'équation s'écrit $3^{2k} - 2^n = 1$. On peut factoriser le terme de gauche comme une différence de carrés :

$$(3^k)^2 - 1^2 = 2^n \implies (3^k - 1)(3^k + 1) = 2^n$$

Les deux facteurs $3^k - 1$ et $3^k + 1$ sont donc des puissances de 2. De plus, la différence entre ces deux facteurs est $(3^k + 1) - (3^k - 1) = 2$. Soit $3^k - 1 = 2^a$ et $3^k + 1 = 2^b$ avec $b > a$. La différence est $2^b - 2^a = 2$. Cela implique $2^a(2^{b-a} - 1) = 2$. La seule façon pour que cette égalité soit vraie est que $2^a = 2$ et $2^{b-a} - 1 = 1$. De $2^a = 2$, on tire $a = 1$. De $2^{b-a} - 1 = 1$, on tire $2^{b-1} = 2$, ce qui donne $b - 1 = 1$, soit $b = 2$. En reportant $a = 1$ dans l'équation $3^k - 1 = 2^a$, on a $3^k - 1 = 2^1 = 2$, ce qui donne $3^k = 3$, donc $k = 1$. Puisque $m = 2k$, on a $m = 2$. Enfin, $n = a + b = 1 + 2 = 3$. La seule solution dans ce cas est le couple $(2, 3)$.

Les seules solutions de l'équation $3^m - 2^n = 1$ sont donc $(1, 1)$ et $(2, 3)$.

Corrigé 3

1. Étude du cycle des puissances de 7 modulo 10.

On calcule :

$$7^2 = 49 \equiv -1 \pmod{10}, \text{ donc } 7^4 \equiv (-1)^2 \equiv 1 \pmod{10}.$$

Ainsi, la suite $(7^n \pmod{10})$ est périodique de période 4. En particulier :

$$7^{4k+r} \equiv 7^r \pmod{10}.$$

2. Réduction de l'exposant 7^7 modulo 4.

Puisque la période est 4, il suffit de déterminer $7^7 \pmod{4}$. Or $7 \equiv -1 \pmod{4}$, donc :

$$7^7 \equiv (-1)^7 \equiv -1 \equiv 3 \pmod{4}.$$

3. Retour au problème initial.

On obtient alors :

$$7^{7^7} \equiv 7^3 \pmod{10}.$$

Mais $7^3 = 343 \equiv 3 \pmod{10}$.

4. Conclusion.

Le dernier chiffre de 7^{7^7} est donc $\boxed{3}$.

Corrigé 4

1. Réduction au cas $a = 2$.

Supposons $a > 2$. On remarque l'identité de factorisation :

$$a^r - 1 = (a - 1)(a^{r-1} + a^{r-2} + \dots + a + 1).$$

Puisque $a - 1 \geq 2$, on obtient une décomposition non triviale de $a^r - 1$, ce qui prouve que $a^r - 1$ n'est pas premier. Ainsi, pour que $a^r - 1$ soit premier, il faut nécessairement que $a = 2$.

2. Réduction au cas où r est premier.

Supposons maintenant que $a = 2$ mais que r n'est pas premier. Alors il existe des entiers $s, t \geq 2$ tels que $r = st$. On peut écrire :

$$2^r - 1 = 2^{st} - 1 = (2^s - 1)(2^{s(t-1)} + 2^{s(t-2)} + \dots + 2^s + 1).$$

On voit donc que $2^r - 1$ est de nouveau factorisé en un produit non trivial, donc n'est pas premier.

3. Conclusion.

On conclut que pour que $a^r - 1$ soit premier, il faut à la fois :

$$a = 2 \quad \text{et} \quad r \text{ premier.}$$

Corrigé 5

On cherche un entier de la forme

$$N = 4 \times \sum_{k=0}^{p-1} 10^k$$

qui soit un multiple de 1996.

Autrement dit, on veut que :

$$1996 \mid 44 \dots 4 \quad (p \text{ fois le chiffre } 4).$$

Cela revient à demander que

$$\frac{44 \dots 4}{1996} \in \mathbb{Z}.$$

Or :

$$44 \dots 4 = 4 \times 11 \dots 1.$$

Donc la condition équivaut à

$$499 \mid 11 \dots 1.$$

Le nombre $11 \dots 1$ (p fois) s'écrit :

$$11 \dots 1 = \frac{10^p - 1}{9}.$$

On doit donc trouver p tel que :

$$499 \mid \frac{10^p - 1}{9}.$$

Comme 499 est premier et $499 \nmid 9$, cela revient à demander :

$$499 \mid 10^p - 1.$$

Par le petit théorème de Fermat : si a est premier avec q , alors $a^{q-1} \equiv 1 \pmod{q}$.

Ici $a = 10$, $q = 499$:

$$10^{498} \equiv 1 \pmod{499}.$$

Donc :

$$10^{498} - 1 \equiv 0 \pmod{499}.$$

Or :

$$10^{498} - 1 = 99 \dots 9 \quad (498 \text{ fois le chiffre } 9),$$

et ce nombre vaut

$$10^{498} - 1 = 9 \times 11 \dots 1 \quad (498 \text{ fois le chiffre } 1).$$

Puisque 499 est premier et ne divise pas 9, on déduit que :

$$499 \mid 11 \dots 1 \quad (498 \text{ chiffres } 1).$$

En multipliant par 4, on obtient le nombre formé de 498 chiffres 4. Ce nombre est divisible par 499, et aussi par 4 (il se termine par un 4).

Comme $\gcd(4, 499) = 1$, il est bien multiple de

$$4 \times 499 = 1996.$$

Conclusion : il existe un multiple de 1996 composé uniquement de chiffres 4, à savoir le nombre formé de 498 chiffres 4.

Corrigé 6

Soit

$$n = \prod_{i=1}^k p_i^{m_i} \quad (p_i \text{ premiers, } m_i \geq 1).$$

Tout diviseur s'écrit $d = \prod_{i=1}^k p_i^{r_i}$ avec $0 \leq r_i \leq m_i$. Le nombre de diviseurs est donc

$$N = \prod_{i=1}^k (m_i + 1).$$

Dans le produit P de tous les diviseurs, l'exposant total de p_i est

$$\sum_{r_i=0}^{m_i} r_i \times \prod_{\substack{j=1 \\ j \neq i}}^k (m_j + 1) = \left(\frac{m_i(m_i+1)}{2} \right) \times \prod_{j \neq i} (m_j + 1) = \frac{m_i}{2} N.$$

Ainsi

$$P = \prod_{i=1}^k p_i^{(m_i/2) N} = \left(\prod_{i=1}^k p_i^{m_i} \right)^{N/2} = n^{N/2}.$$

Corrigé 7

Nous allons démontrer que les seuls polynômes répondant à la condition sont les polynômes de degré 1, de la forme $P(X) = aX + b$ avec $a, b \in \mathbb{Q}$ et $a \neq 0$.

Partie 1 : Vérification de la condition. Considérons un polynôme $P(X) = aX + b$ avec $a \in \mathbb{Q}^*$ et $b \in \mathbb{Q}$. Soit x un nombre irrationnel. Supposons par l'absurde que $P(x)$ est un nombre rationnel, notons-le y . On a alors $ax + b = y$. Comme $a \neq 0$, on peut écrire $x = \frac{y-b}{a}$. Puisque a, b, y sont des rationnels, $\frac{y-b}{a}$ est aussi rationnel. Ceci implique que x est rationnel, ce qui contredit notre hypothèse de départ. Donc, $P(x)$ est nécessairement irrationnel.

Partie 2 : Démonstration par l'absurde. Supposons qu'il existe un polynôme P de degré $n \geq 2$ qui satisfait la condition. Quitte à multiplier P par une constante, on peut supposer ses coefficients entiers :

$$P(X) = \sum_{k=0}^n a_k X^k \text{ avec } a_k \in \mathbb{Z} \text{ et } a_n \neq 0.$$

Soit q un nombre premier. L'équation $P(x) = a_0 + \frac{1}{q}$ a une image rationnelle, donc par hypothèse sa solution x_0 doit être rationnelle. Le théorème des valeurs intermédiaires garantit l'existence d'une telle solution réelle.

Posons $x_0 = \frac{u}{v}$ avec $\gcd(u, v) = 1$. L'équation devient :

$$a_n \left(\frac{u}{v}\right)^n + \dots + a_1 \frac{u}{v} + a_0 = a_0 + \frac{1}{q}$$

En simplifiant et multipliant par $v^n q$, on obtient :

$$q(a_n u^n + a_{n-1} u^{n-1} v + \dots + a_1 u v^{n-1}) = v^n$$

De là, on tire que $q|v^n$, et donc $q|v$. En réécrivant l'équation, on a $a_n u^n + \dots + a_1 u v^{n-1} = \frac{v^n}{q}$. Comme

$n \geq 2$ et $q|v$, le terme $\frac{v^n}{q}$ est divisible par q . Le membre de gauche est donc divisible par q . Dans ce membre, tous les termes sauf $a_n u^n$ sont des multiples de v , donc de q . On en déduit que $q|a_n u^n$.

Puisque $q|v$ et $\gcd(u, v) = 1$, q ne divise pas u . Comme q est premier, il doit diviser a_n .

Conclusion. Ce raisonnement étant valable pour n'importe quel nombre premier q , le coefficient a_n devrait être divisible par tous les nombres premiers, ce qui est impossible pour un entier non nul. L'hypothèse d'un polynôme de degré $n \geq 2$ est donc fausse. Les seules solutions sont les polynômes de degré 1.

Corrigé 8

1. Majoration du module des racines

Soit z une racine de P .

Cas 1 : si $|z| \leq 1$, l'inégalité est immédiatement vérifiée.

Cas 2 : supposons $|z| > 1$. D'après $P(z) = 0$, on a :

$$a_n z^n = - \sum_{k=0}^{n-1} a_k z^k.$$

En prenant les modules et en appliquant l'inégalité triangulaire :

$$|a_n| |z|^n \leq \sum_{k=0}^{n-1} |a_k| |z|^k.$$

En divisant par $|a_n|$ et en majorant chaque rapport $\frac{|a_k|}{|a_n|}$ par M :

$$|z|^n \leq M \sum_{k=0}^{n-1} |z|^k.$$

Or, la somme est une série géométrique :

$$\sum_{k=0}^{n-1} |z|^k = \frac{|z|^n - 1}{|z| - 1}.$$

Donc :

$$|z|^n \leq M \cdot \frac{|z|^n - 1}{|z| - 1}.$$

En divisant par $|z|^n > 0$:

$$1 \leq M \cdot \frac{1 - \frac{1}{|z|^n}}{|z| - 1}.$$

Comme $1 - \frac{1}{|z|^n} < 1$, on obtient :

$$1 < \frac{M}{|z| - 1}.$$

Ce qui équivaut à :

$$|z| - 1 < M \implies |z| < M + 1.$$

En conclusion, pour toute racine z de P :

$$|z| \leq 1 + M.$$

2. Irréductibilité de P

Raisonnons par l'absurde. Supposons que P soit **réductible** dans $\mathbb{Z}[X]$.

Alors, d'après le lemme de Gauss, il existe $Q, R \in \mathbb{Z}[X]$ non constants tels que :

$$P(X) = Q(X)R(X).$$

Or, $P(m)$ est premier. Donc :

$$P(m) = Q(m)R(m).$$

Ainsi, l'un des deux facteurs $Q(m)$ ou $R(m)$ vaut nécessairement ± 1 . Supposons donc :

$$|Q(m)| = 1.$$

Étude de $Q(m)$: Soient $z_1, \dots, z_s$ les racines de Q . Elles sont aussi racines de P , donc d'après la question 1 :

$$|z_i| \leq M + 1.$$

On a, par inégalité triangulaire inversée :

$$|m - z_i| \geq |m| - |z_i|.$$

Comme $m > M+2$ et $|z_i| \leq M+1$, on a $m > |z_i|$, donc :

$$|m - z_i| = m - |z_i| \geq m - (M + 1).$$

Or $m > M + 2$, donc :

$$m - (M + 1) > 1 \quad \implies \quad |m - z_i| > 1.$$

Évaluation de $Q(m)$: On peut écrire :

$$|Q(m)| = |b_s| \prod_{i=1}^s |m - z_i|,$$

où b_s est le coefficient dominant de Q .

Comme $Q \in \mathbb{Z}[X]$, on a $|b_s| \geq 1$, et pour tout i , $|m - z_i| > 1$.

Donc :

$$|Q(m)| > 1.$$

Cela contredit l'hypothèse $|Q(m)| = 1$.

Conclusion : L'hypothèse de réductibilité est donc fausse. Ainsi, P est **irréductible dans $\mathbb{Z}[X]$** .