Arithmétique

Divisibilité

Exercice 1 [01187] [Correction]
Résoudre dans $\mathbb{Z}$ les équations suivantes :
(a) $x-1 \mid x+3$ b) $x+2 \mid x^2+2$.

Exercice 2 [01188] [Correction]
Résoudre dans $\mathbb{Z}^2$ les équations suivantes :

(a) $xy = 3x+2y$ (b) $\frac{1}{x}+\frac{1}{y}=\frac{1}{5}$ (c) $x^2-y^2-4x-2y=5$

Exercice 3 [02358] [Correction]
Pour $n \in \mathbb{N}^*$, on désigne par N le nombre de diviseurs positifs de n et par P leur produit. Quelle relation existe-t-il entre n, N et P ?

Division euclidienne

Exercice 4 [01189] [Correction]
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, on note q le quotient de la division euclidienne de $a-1$ par b.
Déterminer pour tout $n \in \mathbb{N}$, le quotient de la division euclidienne de (ab^n-1) par b^{n+1}.

Exercice 5 [01215] [Correction]
On considère la suite $(\varphi_n)_{n\in\mathbb{N}}$ définie par

$$\varphi_0 = 0, \varphi_1 = 1 \text{ et } \forall n \in \mathbb{N}, \varphi_{n+2} = \varphi_{n+1} + \varphi_n$$

(a) Montrer
$$\forall n \in \mathbb{N}^*, \varphi_{n+1}\varphi_{n-1} - \varphi_n^2 = (-1)^n$$

(b) En déduire
$$\forall n \in \mathbb{N}^*, \varphi_n \wedge \varphi_{n+1} = 1$$

(c) Montrer
$$\forall n \in \mathbb{N}, \forall m \in \mathbb{N}^*, \varphi_{n+m} = \varphi_m\varphi_{n+1} + \varphi_{m-1}\varphi_n$$

(d) En déduire
$$\forall m, n \in \mathbb{N}^*, \text{pgcd}(\varphi_n, \varphi_{m+n}) = \text{pgcd}(\varphi_n, \varphi_m)$$
puis $\text{pgcd}(\varphi_m, \varphi_n) = \text{pgcd}(\varphi_n, \varphi_r)$ où r est le reste de la division euclidienne de m par n.

(e) Conclure
$$\text{pgcd}(\varphi_m, \varphi_n) = \varphi_{\text{pgcd}(m,n)}$$

PGCD et PPCM

Exercice 6 [01195] [Correction]
Déterminer le pgcd et les coefficients de l'égalité de Bézout (1730-1783) des entiers a et b suivants :
(a) $a = 33$ et $b = 24$
(b) $a = 37$ et $b = 27$
(c) $a = 270$ et $b = 105$.

Exercice 7 [01196] [Correction]
Soient $a, b, d \in \mathbb{Z}$. Montrer l'équivalence :

$$(\exists u, v \in \mathbb{Z}, au + bv = d) \iff \text{pgcd}(a, b) \mid d$$

Exercice 8 [01197] [Correction]
Montrer que le pgcd de $2n+4$ et $3n+3$ ne peut être que $1, 2, 3$ ou 6.

Exercice 9 [01199] [Correction]
Soient $d, m \in \mathbb{N}$. Donner une condition nécessaire et suffisante pour que le système

$$\begin{cases} \text{pgcd}(x, y) = d \\ \text{ppcm}(x, y) = m \end{cases}$$

possède un couple $(x, y) \in \mathbb{N}^2$ solution.

Exercice 10 [01200] [Correction]
Résoudre dans $\mathbb{N}^2$ l'équation :

$$\text{pgcd}(x,y) + \text{ppcm}(x,y) = x + y$$

Exercice 11 [01201] [Correction]
Résoudre dans $\mathbb{N}^2$ les systèmes :

(a) $\begin{cases} \text{pgcd}(x,y) = 5 \\ \text{ppcm}(x,y) = 60 \end{cases}$ (b) $\begin{cases} x + y = 100 \\ \text{pgcd}(x,y) = 10 \end{cases}$

Nombres premiers entre eux

Exercice 12 [01203] [Correction]
Soient $a, b \in \mathbb{Z}$.

(a) On suppose $a \wedge b = 1$. Montrer que $(a+b) \wedge ab = 1$.

(b) On revient au cas général. Calculer $\text{pgcd}(a+b, \text{ppcm}(a,b))$.

Exercice 13 [01204] [Correction]
Montrer que pour tout $n \in \mathbb{N}^*$ on a :

(a) $(n^2+n) \wedge (2n+1) = 1$ (b) $(3n^2+2n) \wedge (n+1) = 1$

Exercice 14 [01205] [Correction]
Montrer que pour tout entier $n \in \mathbb{N}^*$, $n+1$ et $2n+1$ sont premiers entre eux.
En déduire

$$n+1 \mid \binom{2n}{n}$$

Exercice 15 [01206] [Correction]
Soient a et b premiers entre eux et $c \in \mathbb{Z}$.
Montrer que $\text{pgcd}(a, bc) = \text{pgcd}(a, c)$.

Exercice 16 [01207] [Correction]
Soient a et b deux entiers premiers entre eux non nuls.
Notre but est de déterminer tous les couples $(u,v) \in \mathbb{Z}^2$ tels que $au + bv = 1$.

(a) Justifier l'existence d'au moins un couple solution (u_0, v_0).

(b) Montrer que tout autre couple solution est de la forme $(u_0 + kb, v_0 - ka)$ avec $k \in \mathbb{Z}$.

(c) Conclure.

Exercice 17 [01208] [Correction]

(a) Pour $n \in \mathbb{N}$, montrer qu'il existe un couple unique $(a_n, b_n) \in \mathbb{N}^2$ tel que

$$(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$$

(b) Calculer $a_n^2 - 2b_n^2$.

(c) En déduire que a_n et b_n sont premiers entre eux.

Exercice 18 [01209] [Correction]
Soient a et b deux entiers relatifs premiers entre eux et $d \in \mathbb{N}$ un diviseur de ab.
Montrer

$$\exists!(d_1,d_2) \in \mathbb{N}^2, d = d_1 d_2, d_1 \mid a \text{ et } d_2 \mid b$$

Exercice 19 [03624] [Correction]
Soit $n \in \mathbb{N}$. Montrer que les entiers

$$a_i = i.n! + 1$$

pour $i \in \{1, \dots, n+1\}$ sont deux à deux premiers entre eux.

Nombres premiers

Exercice 20 [03209] [Correction]
Soient $n \geq 2$ et N la somme de n entiers impairs consécutifs. Montrer que N n'est pas un nombre premier.

Exercice 21 [01219] [Correction]
Montrer que les nombres suivants sont composés :

(a) $4n^3+6n^2+4n+1$ avec $n\in\mathbb{N}^*$ (b) n^4-n^2+16 avec $n\in\mathbb{Z}$.

Exercice 22 [03623] [Correction]
Soit n un naturel non nul. Montrer qu'il existe toujours un nombre premier strictement compris entre n et $n!+2$.

Exercice 23 [01224] [Correction]
Justifier l'existence de 1 000 entiers consécutifs sans nombres premiers.

Exercice 24 [02369] [Correction]
On suppose que n est un entier ≥ 2 tel que 2^n-1 est premier.
Montrer que n est nombre premier.

Exercice 25 [02656] [Correction]
Soient des entiers $a>1$ et $n>0$.
Montrer que si a^n+1 est premier alors n est une puissance de 2.

Exercice 26 [03351] [Correction]
Soient $a,b\in\mathbb{N}\setminus\{0,1\}$ et $n\in\mathbb{N}^*$.
On suppose que a^n+b^n est un nombre premier. Montrer que n est une puissance de 2.

Exercice 27 [01223] [Correction]
Soit $E=\{4k-1\mid k\in\mathbb{N}^*\}$.

(a) Montrer que pour tout $n\in E$, il existe $p\in\mathcal{P}\cap E$ tel que $p\mid n$.

(b) En déduire qu'il y a une infinité de nombre premier p tel que $p=-1 \mod 4$.

Études arithmétiques

Exercice 28 [01225] [Correction]
Soit $n\in\mathbb{N}$, montrer

$$\sqrt{n}\in\mathbb{Q} \iff \exists m\in\mathbb{N}, n=m^2$$

En déduire que $\sqrt{2}\notin\mathbb{Q}$ et $\sqrt{3}\notin\mathbb{Q}$

Exercice 29 [01212] [Correction]
Soit $x\in\mathbb{Q}$. On suppose qu'il existe $n\in\mathbb{N}^*$ tel que $x^n\in\mathbb{Z}$. Montrer que $x\in\mathbb{Z}$.

Exercice 30 [01213] [Correction]
Soient $a,b\in\mathbb{N}^*$. On suppose qu'il existe m,n premiers entre eux tels que $a^m=b^n$.
Montrer qu'il existe $c\in\mathbb{N}^*$ tel que $a=c^n$ et $b=c^m$.

Exercice 31 [01214] [Correction]
On divise un cercle en n arcs égaux et on joint les points de division de p en p jusqu'à ce qu'on revienne au point de départ. Quel est le nombre de côtés du polygone construit ?

Exercice 32 [03669] [Correction]
On étudie l'équation algébrique

$$(E)\colon x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$$

d'inconnue x et où les coefficients $a_0,a_1,\ldots,a_{n-1}$ sont supposés entiers.
Montrer que les solutions réelles de (E) sont entières ou irrationnelles.

Exercice 33 [01228] [Correction]
Soient $p\in\mathcal{P}$ et $\alpha\in\mathbb{N}^*$. Déterminer les diviseurs positifs de p^α.

Exercice 34 [01229] [Correction]
Soit $n\in\mathbb{N}\setminus\{0,1\}$ et $n=\prod_{k=1}^{N}p_k^{\alpha_k}$ sa décomposition primaire.
Quel est le nombre de diviseurs positifs de n ?

Exercice 35 [01230] [Correction]
Soit $n\in\mathbb{N}\setminus\{0,1\}$ dont la décomposition primaire est

$$n=\prod_{i=1}^{N}p_i^{\alpha_i}$$

On note $d(n)$ le nombre de diviseurs supérieurs ou égaux à 1 de n et $\sigma(n)$ la somme de ceux-ci.
Montrer

$$d(n)=\prod_{i=1}^{N}(\alpha_i+1) \text{ et } \sigma(n)=\prod_{i=1}^{N}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

Exercice 36 [01231] [Correction]
Soit $\sigma : \mathbb{Z} \to \mathbb{N}$ qui à $n \in \mathbb{Z}$ associe la somme de diviseurs positifs de n.

(a) Soit $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$. Calculer $\sigma(p^\alpha)$.

(b) Soient $a, b \in \mathbb{Z}$ premiers entre eux.
Montrer que tout diviseur positif d du produit ab s'écrit de manière unique $d = d_1 d_2$ avec d_1 et d_2 diviseurs positifs de a et b.

(c) En déduire que si a et b sont premiers entre eux alors $\sigma(ab) = \sigma(a)\sigma(b)$.

(d) Exprimer $\sigma(n)$ en fonction de la décomposition primaire de n.

Valuation p-adique

Exercice 37 [01226] [Correction]
Pour $p \in \mathcal{P}$ et $n \in \mathbb{Z}$, on note $v_p(n)$ l'exposant de la plus grande puissance de p divisant n.

(a) Montrer que $v_2(1\,000!) = 994$.

(b) Plus généralement, calculer $v_p(n!)$. On rappelle que

$$\forall x \in \mathbb{R}, \left\lfloor \frac{\lfloor px \rfloor}{p} \right\rfloor = \lfloor x \rfloor$$

Exercice 38 [02370] [Correction]
On note $\mathcal{P}$ l'ensemble des nombres premiers. Pour tout entier $n > 0$, on note $v_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers. On note $\lfloor x \rfloor$ la partie entière de x. On note $\pi(x)$ le nombre de nombres premiers au plus égaux à x.

(a) Montrer que $v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.

(b) Montrer que $\binom{2n}{n}$ divise $\prod_{p \in \mathcal{P}; p \leq 2n} p^{\left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor}$.

(c) Montrer que $\binom{2n}{n} \leq (2n)^{\pi(2n)}$.

(d) Montrer que $\frac{x}{\ln x} = \mathrm{O}(\pi(x))$ quand $x \to +\infty$

Petit théorème de Fermat

Exercice 39 [01222] [Correction]
Soit p un nombre premier.

(a) Montrer

$$\forall k \in \{1, 2, \ldots, p-1\}, p \mid \binom{p}{k}$$

(b) En déduire que

$$\forall n \in \mathbb{Z}, n^p \equiv n \mod p$$

Exercice 40 [03636] [Correction]
Soit $n \geq 2$ un entier. On suppose

$$\forall a \in \{1, \ldots, n-1\}, a^{n-1} \equiv 1 \quad [n]$$

Montrer que n est un nombre premier

Exercice 41 [00204] [Correction]
(Nombres de Carmichael) Soit n un entier supérieur à 2.
On suppose que n pour tout facteur premier p de n, p^2 ne divise pas n mais $p-1$ divise $n-1$.
Établir

$$\forall a \in \mathbb{Z}, a^n \equiv a \quad [n]$$

Corrections

Exercice 1 : [énoncé]

(a) $x=1$ n'est pas solution. Pour $x \neq 1$:
$x-1 \mid x+3 \iff \frac{x+3}{x-1} = 1+\frac{4}{x-1} \in \mathbb{Z} \iff x-1 \in \mathcal{D}(4) = \{1,2,4,-1,-2,-4\}$
Ainsi $\mathcal{S} = \{2,3,5,0,-1,-3\}$.

(b) $x=-2$ n'est pas solution. Pour $x \neq -2$:
$x+2 \mid x^2+2 \iff \frac{x^2+2}{x+2} = x-2+\frac{6}{x+2} \in \mathbb{Z} \iff x+2 \in \mathcal{D}(6) = \{1,2,3,6,-1,-2,-3,-6\}$.
Ainsi $\mathcal{S} = \{-1,0,1,4,-3,-4,-5,-8\}$.

Exercice 2 : [énoncé]

(a) On a
$$xy = 3x+2y \iff (x-2)(y-3) = 6$$
En détaillant les diviseurs de 6 possibles, on obtient
$$\mathcal{S} = \{(3,9),(4,6),(5,5),(8,4),(1,-3),(0,0),(-1,1),(-4,2)\}$$

(b) Pour $x,y \in \mathbb{Z}^*$,
$$\frac{1}{x}+\frac{1}{y} = \frac{1}{5} \iff 5x+5y = xy \iff (x-5)(y-5) = 25$$
En détaillant les diviseurs de 25 possibles, on obtient
$$\mathcal{S} = \{(6,30),(10,10),(30,6),(4,-20),(-20,4)\}$$

(c) On a
$$x^2-y^2-4x-2y = 5 \iff (x-2)^2-(y+1)^2 = 8$$
et donc
$$x^2-y^2-4x-2y = 5 \iff (x-y-3)(x+y-1) = 8$$
En détaillant les diviseurs de 8 possibles et sachant
$$\begin{cases} x-y-3 = a \\ x+y-1 = b \end{cases} \iff \begin{cases} x = \frac{a+b}{2}+2 \\ y = \frac{b-a}{2}-1 \end{cases}$$
on obtient
$$\mathcal{S} = \{(5,0),(5,-2),(-1,0),(-1,-2)\}$$

Exercice 3 : [énoncé]
En associant dans $P^2 = P \times P$ chaque diviseur d avec celui qui lui est conjugué n/d, on obtient un produit de N termes égaux à n. Ainsi
$$P^2 = n^N$$

Exercice 4 : [énoncé]
$a-1 = bq+r$ avec $0 \leq r < b$.
$ab^n - 1 = (bq+r+1)b^n - 1 = qb^{n+1} + b^n(r+1) - 1$.
Or $0 \leq b^n(r+1) - 1 < b^{n+1}$ donc la relation ci-dessus est la division euclidienne de $ab^n - 1$ par b^{n+1}.
Le quotient de celle-ci est donc q.

Exercice 5 : [énoncé]

(a) Par récurrence sur $n \in \mathbb{N}^*$:
Pour $n=1$: $\varphi_2\varphi_0 - \varphi_1^2 = 0-1 = -1$: ok.
Supposons la propriété établie au rang $n \geq 1$.
$$\varphi_{n+2}\varphi_n - \varphi_{n+1}^2 = (\varphi_n+\varphi_{n+1})\varphi_n - \varphi_{n+1}(\varphi_n+\varphi_{n-1}) = \varphi_n^2 - \varphi_{n+1}\varphi_{n-1} \underset{HR}{=} -(-1)^n = (-$$
Récurrence établie.

(b) Par l'égalité de Bézout on obtient que $\varphi_n \wedge \varphi_{n+1} = 1$ puisque la relation précédente permet d'écrire $u\varphi_n + v\varphi_{n+1} = 1$ avec $u,v \in \mathbb{Z}$.

(c) Par récurrence sur $m \in \mathbb{N}^*$
Pour $m=1$: $\varphi_{n+1} = \varphi_1\varphi_{n+1} + \varphi_0\varphi_n$ car $\varphi_1 = 1$ et $\varphi_0 = 0$.
Supposons la propriété établie au rang $n \geq 1$
$$\varphi_{n+m+1} = \varphi_{(n+1)+m} \underset{HR}{=} \varphi_m\varphi_{n+2} + \varphi_{m-1}\varphi_{n+1} = \varphi_m\varphi_{n+1} + \varphi_m\varphi_n + \varphi_{m-1}\varphi_{n+1} = \varphi_{m+1}$$
Récurrence établie.

(d)
$$\text{pgcd}(\varphi_{m+n}, \varphi_n) = \text{pgcd}(\varphi_m\varphi_{n-1} + \varphi_{m-1}\varphi_n, \varphi_n) = \text{pgcd}(\varphi_m\varphi_{n-1}, \varphi_n) = \text{pgcd}(\varphi_m, \varphi_n)$$
car $\varphi_n \wedge \varphi_{n-1} = 1$.
Par récurrence on obtient que
$$\forall q \in \mathbb{N} \varphi_m \wedge \varphi_n = \varphi_{m+qn} \wedge \varphi_n$$
On en déduit alors $\text{pgcd}(\varphi_m, \varphi_n) = \text{pgcd}(\varphi_n, \varphi_r)$ car on peut écrire $m = nq+r$ avec $q \in \mathbb{N}$.

(e) Suivons l'algorithme d'Euclide calculant $\text{pgcd}(m,n)$:
$a_0 = m, a_1 = n$, $a_0 = a_1q_1 + a_2$, $a_1 = a_2q_2 + a_3$,..., $a_{p-1} = a_pq_p + 0$ avec $a_p = \text{pgcd}(m,n)$
Or
$\text{pgcd}(\varphi_n, \varphi_m) = \text{pgcd}(\varphi_{a_0}, \varphi_{a_1}) = \text{pgcd}(\varphi_{a_1}, \varphi_{a_2}) = \ldots = \text{pgcd}(\varphi_{a_p}, \varphi_0) = \varphi_{a_p}$
car $\varphi_0 = 0$.
Ainsi $\text{pgcd}(\varphi_m, \varphi_n) = \varphi_{\text{pgcd}(m,n)}$.

Exercice 6 : [énoncé]

(a) $\text{pgcd}(a,b) = 3$ et $3a - 4b = 3$.

(b) $\text{pgcd}(a,b) = 1$ et $11b - 8a = 1$

(c) $\text{pgcd}(a,b) = 15$ et $2a - 5b = 15$

Exercice 7 : [énoncé]
($\Longrightarrow$) Supposons $d = au + bv$ avec $u, v \in \mathbb{Z}$.
$\text{pgcd}(a,b) \mid a$ et $\text{pgcd}(a,b) \mid b$ donc $\text{pgcd}(a,b) \mid au + bv = d$.
($\Longleftarrow$) Supposons $\text{pgcd}(a,b) \mid d$. On peut écrire $d = k\,\text{pgcd}(a,b)$ avec $k \in \mathbb{Z}$.
Par l'égalité de Bézout, il existe $u_0, v_0 \in \mathbb{Z}$ tels que

$$au_0 + bv_0 = \text{pgcd}(a,b)$$

et on a alors

$$d = au + bv$$

avec $u = ku_0$ et $v = kv_0 \in \mathbb{Z}$

Exercice 8 : [énoncé]
$3 \times (2n+4) - 2 \times (3n+3) = 6$ donc $\text{pgcd}(2n+4, 3n+3) \mid 6$.

Exercice 9 : [énoncé]
Si le système possède une solution alors $d \mid m$ est une condition nécessaire.
Inversement si $d \mid m$ alors $x = d$ et $y = m$ donne un couple $(x,y) \in \mathbb{N}^2$ solution.

Exercice 10 : [énoncé]
Soit $(x,y) \in \mathbb{N}^2$ un couple solution. Posons $\delta = \text{pgcd}(x,y)$.
On peut écrire

$$x = \delta x' \text{ et } y = \delta y' \text{ avec } x' \wedge y' = 1$$

L'équation devient :

$$1 + x'y' = x' + y' \iff (x'-1)(y'-1) = 0 \iff x' = 1 \text{ ou } y' = 1$$

Ainsi (x,y) est de la forme $(\delta, \delta k)$ ou $(\delta k, \delta)$ avec $k \in \mathbb{N}$.
Inversement ces couples sont solutions.

Exercice 11 : [énoncé]

(a) Soit (x,y) solution. $\text{pgcd}(x,y) = 5$ donc $x = 5x'$ et $y = 5y'$ avec $x', y' \in \mathbb{N}$ premiers entre eux.
$\text{ppcm}(x,y) = 5x'y' = 60$ donc $x'y' = 12$ d'où

$$(x',y') \in \{(1,12),(2,6),(3,4),(4,3),(6,2),(12,1)\}.$$

Les couples $(2,6)$ et $(6,2)$ sont à éliminer car 2 et 6 ne sont pas premiers entre eux.
Finalement,

$$(x,y) \in \{(5,60),(15,20),(20,15),(60,5)\}.$$

Inversement : ok. Finalement $\mathcal{S} = \{(5,60),(15,20),(20,15),(60,5)\}$.

(b) Soit (x,y) solution. $\text{pgcd}(x,y) = 10$ donc $x = 10x'$ et $y = 10y'$ avec $x', y' \in \mathbb{N}$ premiers entre eux.
$x + y = 10(x' + y') = 100$ donc $x' + y' = 10$.
Sachant $x' \wedge y' = 1$, il reste $(x',y') \in \{(1,9),(3,7),(7,3),(9,1)\}$ puis $(x,y) \in \{(10,90),(30,70),(70,30),(90,10)\}$.
Inversement : ok. Finalement $\mathcal{S} = \{(10,90),(30,70),(70,30),(90,10)\}$.

Exercice 12 : [énoncé]

(a) $\text{pgcd}(a, a+b) = \text{pgcd}(a,b)$ et $\text{pgcd}(b, a+b) = \text{pgcd}(a,b) = 1$.
Ainsi $(a+b) \wedge a = 1$ et $(a+b) \wedge b = 1$ donc $(a+b) \wedge ab = 1$.

(b) Posons $\delta = \text{pgcd}(a,b)$. On peut écrire $a = \delta a'$ et $b = \delta b'$ avec $a' \wedge b' = 1$.
$\text{pgcd}(a+b, \text{ppcm}(a,b)) = \delta\,\text{pgcd}(a'+b', \text{ppcm}(a',b')) = \delta$

Exercice 13 : [énoncé]

(a) $n^2+n=n(n+1)$.
$1\times(2n+1)-2\times n=1$ donc $(2n+1)\wedge n=1$.
$2\times(n+1)-1\times(2n+1)=1$ donc $(2n+1)\wedge(n+1)=1$
Par produit $(2n+1)\wedge(n^2+n)=1$.

(b) $3n^2+2n=n(3n+2)$.
$1\times(n+1)-1\times n=1$ donc $n\wedge(n+1)=1$.
$3\times(n+1)-1\times(3n+2)=1$ donc $(3n+2)\wedge(n+1)=1$.
Par produit $(3n^2+2n)\wedge(n+1)=1$.

Exercice 14 : [énoncé]
$2\times(n+1)-1\times(2n+1)=1$ donc $(n+1)\wedge(2n+1)=1$.
On a

$$\binom{2n+1}{n+1}=\frac{2n+1}{n+1}\binom{2n}{n}$$

donc

$$(n+1)\binom{2n+1}{n+1}=(2n+1)\binom{2n}{n}$$

Puisque $\binom{2n+1}{n+1}\in\mathbb{Z}$, on a

$$(n+1)\mid(2n+1)\binom{2n}{n}$$

or $(n+1)\wedge(2n+1)=1$ donc

$$(n+1)\mid\binom{2n}{n}$$

Exercice 15 : [énoncé]
Posons $d=\text{pgcd}(a,bc)$ et $\delta=\text{pgcd}(a,c)$.
On $\delta\mid a$ et $\delta\mid c$ donc $\delta\mid bc$ puis $\delta\mid d$.
Inversement $d\mid a$ et $d\mid bc$.
Or $d\wedge b=1$ car $d\mid a$ et $a\wedge b=1$. Donc $d\mid c$ puis $d\mid\delta$.
Par double divisibilité $d=\delta$.

Exercice 16 : [énoncé]

(a) Théorème de Bézout.

(b) Soit $(u,v)\in\mathbb{Z}^2$ un couple solution. On a $au+bv=1=au_0+bv_0$ donc $a(u-u_0)=b(v_0-v)$
On a $a\mid b(v_0-v)$ or $a\wedge b=1$ donc $a\mid v_0-v$. Ainsi $\exists k\in\mathbb{Z}$ tel que $v=v_0-ka$ et alors $a(u-u_0)=b(v_0-v)$ donne $a(u-u_0)=abk$ puis $u=u_0+kb$ (sachant $a\neq0$).

(c) Inversement les couples de la forme ci-dessus sont solutions.

Exercice 17 : [énoncé]

(a) Unicité : Si (a_n,b_n) et (α_n,β_n) sont solutions alors

$$a_n+b_n\sqrt{2}=\alpha_n+\beta_n\sqrt{2}$$

donc

$$(b_n-\beta_n)\sqrt{2}=(\alpha_n-a_n)$$

Si $b_n\neq\beta_n$ alors

$$\sqrt{2}=\frac{\alpha_n-a}{b_n-\beta_n}\in\mathbb{Q}$$

ce qui est absurde.
On en déduit $b_n=\beta_n$ puis $a_n=\alpha_n$
Existence : Par la formule du binôme

$$(1+\sqrt{2})^n=\sum_{k=0}^{n}\binom{n}{k}\sqrt{2}^k$$

En séparant les termes d'indices pairs de ceux d'indices impairs, on a

$$(1+\sqrt{2})^n=a_n+b_n\sqrt{2}$$

avec

$$a_n=\sum_{p=0}^{E(n/2)}\binom{n}{2p}2^p \text{ et } b_n=\sum_{p=0}^{E((n-1)/2)}\binom{n}{2p+1}2^p$$

(b) On a

$$a_n^2-2b_n^2=(a_n+b_n\sqrt{2})\left(a_n-b_n\sqrt{2}\right)$$

Or en reprenant les calculs qui précèdent

$$(1-\sqrt{2})^n=a_n-b_n\sqrt{2}$$

donc

$$a_n^2-2b_n^2=(1+\sqrt{2})^n(1-\sqrt{2})^n=(-1)^n$$

(c) La relation qui précède permet d'écrire

$$a_n u + b_n v = 1 \text{ avec } u, v \in \mathbb{Z}$$

On en déduit que a_n et b_n sont premiers entre eux.

Exercice 18 : [énoncé]
Unicité : Si (d_1, d_2) est solution alors $\text{pgcd}(d, a) = \text{pgcd}(d_1 d_2, a)$
Or $d_2 \wedge a = 1$ car $d_2 \mid b$ et $a \wedge b = 1$, donc $\text{pgcd}(d_1 d_2, a) = \text{pgcd}(d_1, a) = d_1$ car $d_1 \mid a$.
De même $d_2 = \text{pgcd}(d, b)$ d'où l'unicité.
Existence : Posons $d_1 = \text{pgcd}(d, a)$ et $d_2 = \text{pgcd}(d, b)$. On a $d_1 \mid a$ et $d_2 \mid b$.
$d_1 \mid a$ et $d_2 \mid b$ donc $d_1 \wedge d_2 = 1$ car $a \wedge b = 1$.
$d_1 \mid d$, $d_2 \mid d$ et $d_1 \wedge d_2 = 1$ donc $d_1 d_2 \mid d$.
Inversement : Par l'égalité de Bézout on peut écrire $d_1 = u_1 d + v_1 a$ et $d_2 = u_2 d + v_2 b$ donc $d \mid d_1 d_2 = U d + v_1 v_2 ab$ car $d \mid ab$.

Exercice 19 : [énoncé]
Par l'absurde, supposons que a_i et a_j (avec $i, j \in \{1, \dots, n+1\}$) ne soient pas premiers entre eux.
Considérons d un diviseur premier commun à a_i et a_j. L'entier d est diviseur de $a_i - a_j$ donc de $(i-j).n!$.
Puisque d est premier et diviseur de $i - j$ ou de $n!$, il est nécessairement inférieur à n et donc assurément diviseur de $n!$. Or d divise aussi $a_i = i.n! + 1$ et donc d divise 1.
C'est absurde.

Exercice 20 : [énoncé]
Notons $2p+1$ le premier nombre impair sommé. On a

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

avec $n \geq 2$ et $n + 2p \geq 2$. Ainsi N est composé.

Exercice 21 : [énoncé]

(a) $4n^3 + 6n^2 + 4n + 1 = (n+1)^4 - n^4 = ((n+1)^2 - n^2)((n+1)^2 + n^2) = (2n+1)(2n^2 + 2n + 1)$.
Cet entier est composé pour $n \in \mathbb{N}^*$ car $2n + 1 \geq 2$ et $2n^2 + 2n + 1 \geq 2$.

(b) $n^4 - n^2 + 16 = (n^2+4)^2 - 9n^2 = (n^2 - 3n + 4)(n^2 + 3n + 4)$.
De plus les équations $n^2 - 3n + 4 = 0, 1$ ou -1 et $n^2 + 3n + 4 = 0,1$ ou -1 n'ont pas de solutions car toutes de discriminant négatif. Par conséquent $n^4 - n^2 + 16$ est composée.

Exercice 22 : [énoncé]
Considérons l'entier $n! + 1$. Celui-ci est divisible par un nombre premier p inférieur à $n! + 1$.
Si ce nombre premier p est aussi inférieur à n alors il divise $n!$ (car apparaît comme l'un des facteurs de ce produit) et donc il divise aussi $1 = (n! + 1) - n!$.
Ceci est absurde et donc le nombre premier en question est au moins égal à $n + 1$.
Finalement, il est strictement compris entre n et $n! + 2$.

Exercice 23 : [énoncé]
Considérons les $x_k = 1001! + k$ avec $2 \leq k \leq 1001$. Ce sont 1 000 entiers consécutifs.
Pour tout $2 \leq k \leq 1001$, on a $k \mid (1001)!$ donc $k \mid x_k$ avec $2 \leq k < x_k$ donc $x_k \notin \mathcal{P}$.

Exercice 24 : [énoncé]
Si $n = ab$ avec $a, b \in \mathbb{N}^*$ alors

$$2^n - 1 = (2^a - 1)(1 + 2^a + \cdots + 2^{a(b-1)})$$

donc $2^a - 1 \mid 2^n - 1$ d'où $2^a - 1 = 1$ ou $2^a - 1 = 2^n - 1$ ce qui implique $a = 1$ ou $a = n$.
Ainsi n ne possède que des diviseurs triviaux, il est premier.

Exercice 25 : [énoncé]
On peut écrire

$$n = 2^k(2p + 1)$$

On a alors

$$a^n + 1 = b^{2p+1} - (-1)^{2p+1} = \big(b - (-1)\big) \sum_{k=0}^{2p} b^k (-1)^{2p-k} = (b+1)c$$

avec $b = a^{2^k}$.
On en déduit que $b + 1 \mid a^n + 1$, or $a^n + 1$ est supposé premier et $b + 1 > 1$ donc $b + 1 = a^n + 1$ puis $n = 2^k$.

Exercice 26 : [énoncé]
On peut écrire $n = 2^k(2p+1)$ avec $k, p \in \mathbb{N}$ et l'enjeu est d'établir $p = 0$.
Posons $\alpha = a^{2^k}$ et $\beta = b^{2^k}$. On a

$$a^n + b^n = \alpha^{2p+1} + \beta^{2p+1} = \alpha^{2p+1} - (-\beta^{2p+1})$$

On peut alors factoriser par $\alpha - (-\beta) = \alpha + \beta$ et puisque $a^n + b^n$ est un nombre premier, on en déduit que $\alpha + \beta = 1$ ou $\alpha + \beta = a^n + b^n$. Puisque $\alpha, \beta \geq 1$, le cas $\alpha + \beta = 1$ est à exclure et puisque $\alpha \leq a^n$ et $\beta \leq b^n$, le cas $\alpha + \beta = a^n + b^n$ entraîne

$$\alpha = a^n \text{ et } \beta = b^n$$

Puisque $a \geq 2$, l'égalité $\alpha = a^n = \alpha^{2p+1}$ entraîne $p = 0$ et finalement n est une puissance de 2.

Exercice 27 : [énoncé]

(a) n est impair, il n'est donc pas divisible par 2. Si tous les nombres premiers p divisant n sont tels que $p = 1 \mod 4$ alors $n = 1 \mod 4$ et donc $n \notin E$

(b) Supposons qu'il n'y ait qu'un nombre fini de nombres premiers $p_1 p_2 \dots p_n$. Considérons

$$n = 4p_1 p_2 \dots p_n - 1 \in E$$

Il existe $p \in \mathcal{P} \cap E$ tel que $p \mid n$ mais $p \mid p_1 p_2 \dots p_n$ donc $p \mid 1$. Absurde.

Exercice 28 : [énoncé]
$(\Longleftarrow)$ ok
$(\Longrightarrow)$ Si $\sqrt{n} \in \mathbb{Q}$ alors on peut écrire $\sqrt{n} = \frac{p}{q}$ avec $p \wedge q = 1$.
On a alors $q^2 n = p^2$ donc $n \mid p^2$
De plus $q^2 n = p^2$ et $p^2 \wedge q^2 = 1$ donne $p^2 \mid n$.
Par double divisibilité $n = p^2$.
ni 2, ni 3 ne sont des carrés d'un entier, donc $\sqrt{2} \notin \mathbb{Q}$ et $\sqrt{3} \notin \mathbb{Q}$.

Exercice 29 : [énoncé]
On peut écrire $x = \frac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et $p \wedge q = 1$.
$x^n = k \in \mathbb{Z}$ donne $q^n k = p^n$. $p \wedge q = 1$ donc $p^n \wedge q^n = 1$. Puisque $q^n \mid p^n \times 1$ on a $q^n \mid 1$ (par Gauss).
Par suite $q^n = 1$ et donc $q = 1$ et $x = p \in \mathbb{Z}$.

Exercice 30 : [énoncé]
Il existe $u, v \in \mathbb{Z}$ tel que $mu + nv = 1$.
Analyse : Si c convient alors $c = c^{mu+nv} = b^u a^v$. *A priori* $c \in \mathbb{Q}$.
Synthèse : Soit $c = b^u a^v$. On a $c^n = b^{nu} a^{nv} = a^{mu} a^{nv} = a$ et de même $c^m = b$.
Puisque le nombre rationnel c possède une puissance entière, $c \in \mathbb{Z}$.

Exercice 31 : [énoncé]
Le nombre de côté du polygone construit est le plus petit entier $k \in \mathbb{N}^*$ tel que $n \mid kp$.
Posons $\delta = \text{pgcd}(n, p)$. On peut écrire $n = \delta n'$ et $p = \delta p'$ avec $n' \wedge p' = 1$.
$n \mid kp \iff n' \mid kp'$ *i.e.* $n' \mid k$. Ainsi $k = n' = n/\delta$.

Exercice 32 : [énoncé]
Supposons $x = p/q$ une racine rationnelle de l'équation (E) avec p et q premiers entre eux.
En réduisant au même dénominateur, on obtient

$$p^n + a_{n-1} q p^{n-1} + \dots + a_1 p q^{n-1} + a_0 q^n = 0$$

Puisque q divise $a_{n-1} q p^{n-1} + \dots + a_1 p q^{n-1} + a_0 q^n$, on obtient que q divise p^n.
Or p et q sont premiers entre eux donc nécessairement $q = 1$ et donc $x = p \in \mathbb{Z}$.
Ainsi les racines rationnelles de (E) sont entières.

Exercice 33 : [énoncé]
Soit $d \in Div(p^\alpha) \cap \mathbb{N}$. Notons β la plus grande puissance de p telle que $p^\beta \mid d$.
On peut écrire $d = p^\beta k$ avec $p \not| k$.
Puisque $p \not| k$ et $p \in \mathcal{P}$ on a $p \wedge k = 1$. Or $k \mid p^\alpha \times 1$ donc, par Gauss : $k \mid 1$.
Par suite $d = p^\beta$ avec $\beta \in \mathbb{N}$. De plus $d \mid p^\alpha$ donc $p^\beta \leq p^\alpha$ puis $\beta \leq \alpha$.
Inversement : ok.

Exercice 34 : [énoncé]
Les diviseurs positifs sont les $d = \prod_{k=1}^N p_k^{\beta_k}$ avec $\forall 1 \leq k \leq N, 0 \leq \beta_k \leq \alpha_k$.
Le choix des β_k conduisant à des diviseurs distincts, il y a exactement $\prod_{k=1}^N (\alpha_k + 1)$ diviseurs positifs de n.

Exercice 35 : [énoncé]
Soit $d \in \mathbb{N}$ diviseur de n.
Tout diviseur premier de d est aussi diviseur de n et c'est donc l'un des $p_1, \dots, p_N$.
Par suite, on peut écrire $d = \prod_{i=1}^{N} p_i^{\beta_i}$ avec $\beta_i \in \mathbb{N}$.
$p_i^{\beta_i} \mid d$ donc $p_i^{\beta_i} \mid n$ d'où $\beta_i \leq \alpha_i$.
Ainsi d est de la forme $d = \prod_{i=1}^{N} p_i^{\beta_i}$ avec pour tout $i \in \{1, \dots, N\}$, $0 \leq \beta_i \leq \alpha_i$.
Inversement de tels nombres sont bien diviseurs de n.
Il y a autant de nombres de cette forme distincts que de choix pour les $\beta_1, \dots, \beta_N$.Pour β_i, il y a $\alpha_i + 1$ choix possibles, au total $d(n) = \prod_{i=1}^{N} (\alpha_i + 1)$.
De plus

$$\begin{aligned}\sigma(n) &= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \dots \sum_{\beta_N=0}^{\alpha_N} p_1^{\beta_1} p_2^{\beta_2} \dots p_N^{\beta_N} \\ &= \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1}\right)\left(\sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2}\right) \dots \left(\sum_{\beta_N=0}^{\alpha_N} p_N^{\beta_N}\right)\end{aligned}$$

Par sommation géométrique

$$\sigma(n) = \prod_{i=1}^{N} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

Exercice 36 : [énoncé]

(a) $Div(p^\alpha) \cap \mathbb{N} = \{1, p, p^2, \dots, p^\alpha\}$ donc $\sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}$.

(b) Soit $d \in Div(ab) \cap \mathbb{N}$. Posons $d_1 = \text{pgcd}(d, a)$ et $d_2 = \text{pgcd}(d, b)$.
On a $d_1 \in Div(a) \cap \mathbb{N}$ et $d_2 \in Div(b) \cap \mathbb{N}$.
Puisque $a \wedge b = 1$ on a $d_1 \wedge d_2 = 1$. Or $d_1 \mid d$ et $d_2 \mid d$ donc $d_1 d_2 \mid d$.
$d_1 = du_1 + av_1$ et $d_2 = du_2 + bv_2$ donc $d_1 d_2 = dk + abv_1 v_2$ d'où $d \mid d_1 d_2$.
Finalement $d = d_1 d_2$.
Supposons $d = \delta_1 \delta_2$ avec $\delta_1 \in Div(a) \cap \mathbb{N}$ et $\delta_2 \in Div(b) \cap \mathbb{N}$.
On a $d_1 \mid \delta_1 \delta_2$ et $d_1 \wedge \delta_2 = 1$ donc $d_1 \mid \delta_1$ et de même $\delta_1 \mid d_1$ puis $d_1 = \delta_1$. De même $d_2 = \delta_2$.

(c) $\sigma(ab) = \sum_{d \mid ab} d = \sum_{d_1 \mid a} \sum_{d_2 \mid b} d_1 d_2 = \left(\sum_{d_1 \mid a} d_1\right)\left(\sum_{d_2 \mid b} d_b\right) = \sigma(a)\sigma(b)$.

(d) Si $n = p_1^{\alpha_1} \dots p_N^{\alpha_N}$ alors $\sigma(n) = \prod_{i=1}^{N} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$.

Exercice 37 : [énoncé]

(a) $v_2(1\,000!) = 500 + v_2(500!)$ car $1000! = 2^{500} \times 500! \times k$ avec k produit de nombres impairs.
$v_2(1\,000!) = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994$.

(b) En isolant les multiples de p dans le produit décrivant $p!$, on obtient

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + v_p\left(\left\lfloor \frac{n}{p} \right\rfloor !\right)$$

puis

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{\lfloor n/p \rfloor}{p} \right\rfloor + v_p\left(\left\lfloor \frac{\lfloor n/p \rfloor}{p} \right\rfloor !\right)$$

or

$$\left\lfloor \frac{\lfloor px \rfloor}{p} \right\rfloor = \lfloor x \rfloor$$

avec $x = n/p^2$ donne

$$\left\lfloor \frac{\lfloor n/p \rfloor}{p} \right\rfloor = \left\lfloor \frac{n}{p^2} \right\rfloor$$

puis finalement

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots + \left\lfloor \frac{n}{p^k} \right\rfloor$$

avec

$$k = \left\lfloor \frac{\ln n}{\ln p} \right\rfloor$$

Exercice 38 : [énoncé]

(a) Pour k suffisamment grand $\lfloor n/p^k \rfloor = 0$, la somme évoquée existe donc car elle ne comporte qu'un nombre fini de termes non nuls. $n! = 1 \times 2 \times \dots \times n$, parmi les entiers allant de 1 à n, il y en a exactement $\lfloor n/p \rfloor$ divisibles par p, $\lfloor n/p^2 \rfloor$ divisibles par p^2, etc... donc

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

(b) On a

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$$

Pour tout $p \in \mathcal{P}$,

$$v_p\left(\frac{(2n)!}{(n!)^2}\right) = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor\right)$$

or $\lfloor 2x\rfloor - 2\lfloor x\rfloor = 0$ ou 1 donc

$$\sum_{k=1}^{\infty}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right) \leq \text{Card}\left\{k\in\mathbb{N}^*/\left\lfloor 2n \mid p^k\right\rfloor > 0\right\} \leq \left\lfloor\frac{\ln(2n)}{\ln p}\right\rfloor$$

De plus les nombres premiers diviseurs de $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ sont diviseurs d'un entier inférieur à $2n$ (lemme d'Euclide) et sont donc eux-mêmes inférieur à $2n$. Il en découle

$$\binom{2n}{n} \mid \prod_{p\in\mathcal{P};p\leq 2n} p^{\left\lfloor\frac{\ln(2n)}{\ln p}\right\rfloor}$$

car toutes les puissances de nombres premiers intervenant dans la décomposition de $\binom{2n}{n}$ divisent $\prod_{p\in\mathcal{P};p\leq 2n} p^{\left\lfloor\frac{\ln(2n)}{\ln p}\right\rfloor}$.
Notons qu'en fait ce produit désigne

$$\text{ppcm}(1,2,\ldots,2n)$$

(c) On a

$$\binom{2n}{n} \leq \prod_{p\in\mathcal{P};p\leq 2n} p^{\left[\frac{\ln(2n)}{\ln p}\right]} \leq \prod_{p\in\mathcal{P};p\leq 2n} p^{\frac{\ln(2n)}{\ln p}} \leq \prod_{p\in\mathcal{P};p\leq 2n} (2n) = (2n)^{\pi(2n)}$$

(d) En passant au logarithme :

$$\sum_{k=1}^{2n}\ln k - 2\sum_{k=1}^{n}\ln k \leq \pi(2n)\ln(2n)$$

À l'aide d'une comparaison intégrale on obtient

$$\int_1^n \ln(t)\,\mathrm{d}t \leq \sum_{k=1}^{n}\ln k \leq \int_1^{(n+1)}\ln(t)\,\mathrm{d}t$$

donc

$$n\ln n - n + 1 \leq \sum_{k=1}^{n}\ln k \leq (n+1)\ln(n+1) - n$$

donc

$$\sum_{k=1}^{n}\ln k = n\ln n - n + \mathrm{O}(\ln n)$$

Par suite

$$\sum_{k=1}^{2n}\ln k - 2\sum_{k=1}^{n}\ln k = 2n\ln(2n) - 2n - 2(n\ln n - n) + \mathrm{O}(\ln n)$$

puis

$$\sum_{k=1}^{2n}\ln k - 2\sum_{k=1}^{n}\ln k \sim \ln(2)(2n)$$

On en déduit

$$\frac{2n}{\ln 2n} = \mathrm{O}(\pi(2n))$$

Ajoutons

$$\frac{x}{\ln x} \sim \frac{2\lfloor x/2\rfloor}{\ln 2\lfloor x/2\rfloor}$$

par calculs et $\pi(x) \sim \pi(2\lfloor x/2\rfloor)$ car $\pi(x)$ et $\pi(2\lfloor x/2\rfloor)$ ne différent qu'au plus d'une unité et $\pi(x)\to+\infty$.
Finalement, une certaine satisfaction.

Exercice 39 : [énoncé]

(a) On a

$$\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$$

donc

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

Par suite $p \mid k\binom{p}{k}$.
Or p est premier et $k < p$ donc $k\wedge p = 1$ puis $p \mid \binom{p}{k}$ en vertu du théorème de Gauss.

(b) Par récurrence finie sur $n\in\{0,1,\ldots,p-1\}$
Pour $n = 0$: ok
Supposons la propriété établie au rang $n\in\{0,1,\ldots,p-2\}$
Par la formule du binôme

$$(n+1)^p = n^p + \sum_{k=1}^{p-1}\binom{p}{k}n^k + 1 \equiv n+1 \mod p$$

car pour $1\leq k\leq p-1$.

$$\binom{p}{k} \equiv 0 \mod p$$

Récurrence établie.
Pour tout $n\in\mathbb{Z}$, il existe $r\in\{0,1,\ldots,p-1\}$ tel que $n\equiv r \quad [p]$ et

$$n^p \equiv r^p \equiv r \equiv n \mod p$$

Exercice 40 : [énoncé]
Pour tout $a \in \{1, \dots, n-1\}$, a est premier avec n. En effet, un diviseur commun à a et n est diviseur de $a^{n-1} - 1$ et donc de 1.
On en déduit que n est premier puisque premier avec chaque naturel strictement inférieur à lui-même.

Exercice 41 : [énoncé]
Par hypothèse, on peut écrire $n = p_1 p_2 \dots p_r$ avec $p_1, \dots, p_r$ nombres premiers deux à deux distincts.
Soit $a \in \mathbb{Z}$. Considérons $i \in \{1, \dots, r\}$.
Si p_i ne divise pas a, le petit théorème de Fermat assure $a^{p_i - 1} \equiv 1 \quad [p_i]$.
Puisque $p_i - 1$ divise $n - 1$, on a encore $a^{n-1} \equiv 1 \quad [p_i]$ et donc $a^n \equiv a \quad [p_i]$
Si p_i divise a alors p_i divise aussi a^n et donc $a^n \equiv 0 \equiv a \quad [p_i]$.
Enfin, chaque p_i divisant $a^n - a$ et les p_i étant deux à deux premiers entre eux, $n = p_1 \dots p_r$ divise $a^n - a$ et finalement $a^n \equiv a \quad [n]$.
La réciproque de ce résultat est vraie.
Ce résultat montre que le petit théorème de Fermat ne caractérise pas les nombres premiers. Les nombres non premiers satisfaisant le petit théorème de Fermat, sont les nombres de Carmichael. Le plus petit d'entre eux est 561, le suivant 1105.