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 :

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

Exercice 3 [00155] [correction]
Soit A un ensemble de $n+1 \geqslant 2$ entiers distincts tous inférieurs ou égaux à $2n$.
Montrer qu'il existe deux éléments de A tels que l'un divise l'autre.

Exercice 4 [02358] [correction]
Pour $n \in \mathbb{N}^\star$, 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 5 [01189] [correction]
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^\star$, 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 6 [01198] [correction]
a) Montrer que si r est le reste de la division euclidienne de $a \in \mathbb{N}$ par $b \in \mathbb{N}^\star$ alors 2^r-1 est le reste de la division euclidienne de 2^a-1 par 2^b-1.
b) Montrer que $\text{pgcd}(2^a-1, 2^b-1) = 2^{\text{pgcd}(a,b)}-1$.

Exercice 7 [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

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

b) En déduire

$$\forall n \in \mathbb{N}^\star,\ \varphi_n \wedge \varphi_{n+1} = 1$$

c) Montrer

$$\forall n \in \mathbb{N}, \forall m \in \mathbb{N}^\star,\ \varphi_{n+m} = \varphi_m\varphi_{n+1}+\varphi_{m-1}\varphi_n$$

d) En déduire

$$\forall m, n \in \mathbb{N}^\star,\ \text{pgcd}(\varphi_n, \varphi_{m+n}) = \text{pgcd}(\varphi_n, \varphi_m)$$

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 8 [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 9 [01196] [correction]
Soient $a, b, d \in \mathbb{Z}$. Montrer l'équivalence :

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

Exercice 10 [01197] [correction]
Montrer que le pgcd de $2n+4$ et $3n+3$ ne peut être que $1, 2, 3$ ou 6.

Exercice 11 [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 12 [01200] [correction]
Résoudre dans $\mathbb{N}^2$ l'équation :

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

Exercice 13 [01201] [correction]
Résoudre dans $\mathbb{N}^2$ les systèmes :

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

Nombres premiers entre eux

Exercice 14 [01202] [correction]
Soient a et b premiers entre eux.
Montrer que $a \wedge (a+b) = b \wedge (a+b) = 1$ puis $(a+b) \wedge ab = 1$.

Exercice 15 [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 16 [01204] [correction]
Montrer que pour tout $n \in \mathbb{N}^\star$ on a :

$$\text{a) } (n^2+n) \wedge (2n+1) = 1 \quad \text{b) } (3n^2+2n) \wedge (n+1) = 1$$

Exercice 17 [01205] [correction]
Montrer que pour tout entier $n \in \mathbb{N}^\star$, $n+1$ et $2n+1$ sont premiers entre eux.
En déduire

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

Exercice 18 [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 19 [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 20 [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 21 [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 22 [01210] [correction]
On note $\text{div}(n)$ l'ensemble des diviseurs positifs d'un entier $n \in \mathbb{Z}$.
Soient $a, b \in \mathbb{Z}$ premiers entre eux et $\varphi : \text{div}(a) \times \text{div}(b) \to \mathbb{N}$ définie par $\varphi(k, \ell) = k\ell$.
Montrer que φ réalise une bijection de $\text{div}(a) \times \text{div}(b)$ vers $\text{div}(ab)$.

Exercice 23 [03624] [correction]
Soit $n \in \mathbb{N}$. Montrer que les entiers
$$a_i = i.n! + 1$$
pour $i \in \{1, \ldots, n+1\}$ sont deux à deux premiers entre eux.

Nombres premiers

Exercice 24 [03209] [correction]
Soient $n \geqslant 2$ et N la somme de n entiers impairs consécutifs. Montrer que N n'est pas un nombre premier.

Exercice 25 [01219] [correction]
Montrer que les nombres suivants sont composés :
a) $4n^3 + 6n^2 + 4n + 1$ avec $n \in \mathbb{N}^\star$ b) $n^4 - n^2 + 16$ avec $n \in \mathbb{Z}$.

Exercice 26 [03623] [correction]
Soit n un naturel non nul. Montrer qu'il existe toujours un nombre premier strictement compris entre n et $n! + 2$.

Exercice 27 [01224] [correction]
Justifier l'existence de 1000 entiers consécutifs sans nombres premiers.

Exercice 28 [02653] [correction]
Soit p un nombre premier, $p \geqslant 5$. Montrer que $p^2 - 1$ est divisible par 24.

Exercice 29 [02369] [correction]
On suppose que n est un entier $\geqslant 2$ tel que $2^n - 1$ est premier.
Montrer que n est nombre premier.

Exercice 30 [01220] [correction]
Soient a et p deux entiers supérieurs à 2.
Montrer que si $a^p - 1$ est premier alors $a = 2$ et p est premier.

Exercice 31 [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 32 [03351] [correction]
Soient $a, b \in \mathbb{N} \backslash \{0, 1\}$ et $n \in \mathbb{N}^\star$.
On suppose que $a^n + b^n$ est un nombre premier. Montrer que n est une puissance de 2.

Exercice 33 [01223] [correction]
Soit $E = \{4k - 1/k \in \mathbb{N}^\star\}$.
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 $p = -1 \quad [4]$.

Exercice 34 [02654] [correction]
Montrer qu'il existe une infinité de nombres premiers de la forme $4n + 3$.

Exercice 35 [02657] [correction]
Soit, pour $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$.
a) Montrer, si $(n, m) \in \mathbb{N}^2$ avec $n \neq m$, que $F_n \wedge F_m = 1$.
b) Retrouver à l'aide du a) le fait que l'ensemble des nombres premiers est infini.

Etudes arithmétiques

Exercice 36 [01225] [correction]
Soit $n \in \mathbb{N}$, montrer
$$\sqrt{n} \in \mathbb{Q} \Leftrightarrow \exists m \in \mathbb{N}, n = m^2$$
En déduire que $\sqrt{2} \notin \mathbb{Q}$ et $\sqrt{3} \notin \mathbb{Q}$

Exercice 37 [01211] [correction]
Soient a et b deux entiers relatifs tels que $a^2 \mid b^2$. Montrer que $a \mid b$.

Exercice 38 [01212] [correction]
Soit $x \in \mathbb{Q}$. On suppose qu'il existe $n \in \mathbb{N}^\star$ tel que $x^n \in \mathbb{Z}$. Montrer que $x \in \mathbb{Z}$.

Exercice 39 [01213] [correction]
Soient $a, b \in \mathbb{N}^\star$. On suppose qu'il existe m, n premiers entre eux tels que $a^m = b^n$.
Montrer qu'il existe $c \in \mathbb{N}^\star$ tel que $a = c^n$ et $b = c^m$.

Exercice 40 [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 41 [03669] [correction]
On étudie l'équation algébrique

$$(E) : x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

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 42 [02361] [correction]
Soit $P \in \mathbb{Z}[X]$ et a, b deux entiers relatifs avec $b > 0$ et $\sqrt{b}$ irrationnel.
a) Exemple : montrer que $\sqrt{6}$ est irrationnel.
b) Quelle est la forme de $(a + \sqrt{b})^n$?
c) Montrer que si $a + \sqrt{b}$ est racine de P alors $a - \sqrt{b}$ aussi.
d) On suppose que $a + \sqrt{b}$ est racine double de P. Montrer que $P = RQ^2$ avec R et Q dans $\mathbb{Z}[X]$.

Exercice 43 [03681] [correction]
On note $d(n)$ le nombre de diviseurs positifs de $n \in \mathbb{N}^\star$.
Déterminer un équivalent de

$$\frac{1}{n}\sum_{k=1}^{n} d(k)$$

représentant la moyenne du nombre de diviseurs positifs des entiers inférieurs à n.

Exercice 44 [01227] [correction]
Soit $n \in \mathbb{N}\backslash\{0, 1\}$. Montrer que n est le produit de ses diviseurs non triviaux si, et seulement si, $n = p^3$ avec $p \in \mathcal{P}$ ou $n = p_1 p_2$ avec $p_1, p_2 \in \mathcal{P}$ distincts.

Exercice 45 [01228] [correction]
Soient $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^\star$. Déterminer les diviseurs positifs de p^α.

Exercice 46 [01229] [correction]
Soit $n \in \mathbb{N}\backslash\{0, 1\}$ et $n = \prod_{k=1}^{N} p_k^{\alpha_k}$ sa décomposition primaire.
Quel est le nombre de diviseurs positifs de n ?

Exercice 47 [01230] [correction]
Soit $n \in \mathbb{N}\backslash\{0, 1\}$ 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 48 [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 $\alpha \in \mathbb{N}^\star$. 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.

Exercice 49 [03725] [correction]
[Théorème d'Aubry]
Soit N un entier strictement positif.
On suppose que le cercle d'équation $x^2 + y^2 = N$ possède un point rationnel (x_0, y_0).
On introduit (x_0', y_0') un point entier obtenu par arrondi de (x_0, y_0).
En étudiant l'intersection du cercle avec la droite joignant (x_0, y_0) et (x_0', y_0'), montrer que le cercle contient un point entier (x_1, y_1).

Valuation p-adique

Exercice 50 [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 $v_2(1000!) = 994$.
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 51 [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 $\prod_{p \in \mathcal{P}; p \leqslant 2n} p^{\left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor}$.
c) Montrer que $\binom{2n}{n} \leqslant (2n)^{\pi(2n)}$.
d) Montrer que $\frac{x}{\ln x} = O(\pi(x))$ quand $x \to +\infty$

Petit théorème de Fermat

Exercice 52 [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

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

Exercice 53 [03636] [correction]
Soit $n \geqslant 2$ 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 54 [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 $n-1$.
Etablir

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

Exercice 55 [03686] [correction]
On désire établir qu'il existe une infinité de nombres premiers de la forme $4n+1$.
Pour cela on raisonne par l'absurde et on suppose que ceux-ci sont en nombre fini et on les numérote pour former la liste $p_1, \ldots, p_r$.
On pose alors

$$N = (2p_1 \ldots p_r)^2 + 1$$

a) On suppose qu'il existe un facteur premier q de N de la forme $4n+3$.
Etablir

$$(2p_1 \ldots p_r)^{(q-1)} \equiv -1 \quad [q]$$

b) Conclure en exploitant le petit théorème de Fermat.

Corrections

Exercice 1 : [énoncé]
a) $x = 1$ n'est pas solution. Pour $x \neq 1$:
$x - 1 \mid x + 3 \Leftrightarrow \frac{x+3}{x-1} = 1 + \frac{4}{x-1} \in \mathbb{Z} \Leftrightarrow x - 1 \in \mathrm{Div}(4) = \{1, 2, 4, -1, -2, -4\}$
Ainsi $\mathcal{S} = \{2, 3, 5, 0, -1, -3\}$.
b) $x = -2$ n'est pas solution. Pour $x \neq -2$:
$x + 2 \mid x^2 + 2 \Leftrightarrow \frac{x^2+2}{x+2} = x - 2 + \frac{6}{x+2} \in \mathbb{Z} \Leftrightarrow x + 2 \in \mathrm{Div}(6) = \{1, 2, 3, 6, -1, -2, -3, -6\}$.
Ainsi $\mathcal{S} = \{-1, 0, 1, 4, -3, -4, -5, -8\}$.

Exercice 2 : [énoncé]
a) On a

$$xy = 3x + 2y \Leftrightarrow (x - 2)(y - 3) = 6$$

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 $x, y \in \mathbb{Z}^\star$,

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{5} \Leftrightarrow 5x + 5y = xy \Leftrightarrow (x - 5)(y - 5) = 25$$

En détaillant les diviseurs de 25 possibles, on obtient

$$\mathcal{S} = \{(6, 30), (10, 10), (30, 6), (4, -20), (-20, 4)\}$$

c) On a

$$x^2 - y^2 - 4x - 2y = 5 \Leftrightarrow (x - 2)^2 - (y + 1)^2 = 8$$

et donc

$$x^2 - y^2 - 4x - 2y = 5 \Leftrightarrow (x - y - 3)(x + y - 1) = 8$$

En détaillant les diviseurs de 8 possibles et sachant

$$\begin{cases} x - y - 3 = a \\ x + y - 1 = b \end{cases} \Leftrightarrow \begin{cases} x = \dfrac{a+b}{2} + 2 \\ y = \dfrac{b-a}{2} - 1 \end{cases}$$

on obtient

$$\mathcal{S} = \{(5, 0), (5, -2), (-1, 0), (-1, -2)\}$$

Exercice 3 : [énoncé]
Les entiers m compris entre 1 et $2n$ peuvent s'écrire $m = 2^k p$ avec p impair compris entre 1 et $2n$.
Il y a exactement n entiers impairs possible entre 1 et $2n$. Pour les $n + 1$ entiers considérés, il y en a donc au moins 2 pour lesquels la valeur de p est la même. Ils s'écrivent $2^k p$ et $2^\ell p$.
Le plus petit des deux divise l'autre.

Exercice 4 : [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 5 : [énoncé]
$a - 1 = bq + r$ avec $0 \leqslant r < b$.
$ab^n - 1 = (bq + r + 1)b^n - 1 = qb^{n+1} + b^n(r + 1) - 1$.
Or $0 \leqslant b^n(r + 1) - 1 < b^{n+1}$ 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 6 : [énoncé]
a) On a$a = bq + r$ avec $0 \leqslant r < b$.

$$2^a - 1 = 2^{bq+r} - 1 = 2^{bq+r} - 2^r + 2^r - 1 = (2^b - 1)(1 + 2^b + \cdots + 2^{b(q-1)})2^r + 2^r - 1$$

avec $0 \leqslant 2^r - 1 < 2^b - 1$.
b) Posons $a_0 = a$, $a_1 = b$ et définissons $a_2, \ldots, a_m$ comme par l'algorithme d'Euclide avec $a_m = \mathrm{pgcd}(a_{m-1}, a_{m-2})$.
On a

$$\mathrm{pgcd}(2^a - 1, 2^b - 1) = \mathrm{pgcd}(2^{a_0} - 1, 2^{a_1} - 1) = \mathrm{pgcd}(2^{a_1} - 1, 2^{a_2} - 1) = \ldots = \mathrm{pgcd}(2^{a_m} - 1, 2^0 - 1$$

Exercice 7 : [énoncé]
a) Par récurrence sur $n \in \mathbb{N}^\star$:
Pour $n = 1$: $\varphi_2\varphi_0 - \varphi_1^2 = 0 - 1 = -1$: ok.
Supposons la propriété établie au rang $n \geqslant 1$.

$$\varphi_{n+2}\varphi_n - \varphi_{n+1}^2 = (\varphi_n + \varphi_{n+1})\varphi_n - \varphi_{n+1}(\varphi_n + \varphi_{n-1}) = \varphi_n^2 - \varphi_{n+1}\varphi_{n-1} \underset{HR}{=} -(-1)^n = (-1)^{n+1}$$

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 $m \in \mathbb{N}^\star$
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 $n \geqslant 1$

$$\varphi_{n+m+1} = \varphi_{(n+1)+m} \underset{HR}{=} \varphi_m\varphi_{n+2} + \varphi_{m-1}\varphi_{n+1} = \varphi_m\varphi_{n+1} + \varphi_m\varphi_n + \varphi_{m-1}\varphi_{n+1} = \varphi_{m+1}\varphi_{n+1} + \varphi_m\varphi_n$$

Récurrence établie.
d)

$$\mathrm{pgcd}(\varphi_{m+n}, \varphi_n) = \mathrm{pgcd}(\varphi_m\varphi_{n-1} + \varphi_{m-1}\varphi_n, \varphi_n) = \mathrm{pgcd}(\varphi_m\varphi_{n-1}, \varphi_n) = \mathrm{pgcd}(\varphi_m, \varphi_n)$$

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 $\mathrm{pgcd}(\varphi_m, \varphi_n) = \mathrm{pgcd}(\varphi_n, \varphi_r)$ car on peut écrire $m = nq + r$ avec $q \in \mathbb{N}$.
e) Suivons l'algorithme d'Euclide calculant $\mathrm{pgcd}(m, n)$:
$a_0 = m, a_1 = n$, $a_0 = a_1q_1 + a_2$, $a_1 = a_2q_2 + a_3$,..., $a_{p-1} = a_pq_p + 0$ avec $a_p = \mathrm{pgcd}(m, n)$
Or $\mathrm{pgcd}(\varphi_n, \varphi_m) = \mathrm{pgcd}(\varphi_{a_0}, \varphi_{a_1}) = \mathrm{pgcd}(\varphi_{a_1}, \varphi_{a_2}) = \ldots = \mathrm{pgcd}(\varphi_{a_p}, \varphi_0) = \varphi_{a_p}$ car $\varphi_0 = 0$.
Ainsi $\mathrm{pgcd}(\varphi_m, \varphi_n) = \varphi_{\mathrm{pgcd}(m,n)}$.

Exercice 8 : [énoncé]
a) $\mathrm{pgcd}(a, b) = 3$ et $3a - 4b = 3$.
b) $\mathrm{pgcd}(a, b) = 1$ et $11b - 8a = 1$
c) $\mathrm{pgcd}(a, b) = 15$ et $2a - 5b = 15$

Exercice 9 : [énoncé]
$(\Rightarrow)$ Supposons $d = au + bv$ avec $u, v \in \mathbb{Z}$.
$\mathrm{pgcd}(a, b) \mid a$ et $\mathrm{pgcd}(a, b) \mid b$ donc $\mathrm{pgcd}(a, b) \mid au + bv = d$.
$(\Leftarrow)$ Supposons $\mathrm{pgcd}(a, b) \mid d$. On peut écrire $d = k\mathrm{pgcd}(a, b)$ avec $k \in \mathbb{Z}$.
Par l'égalité de Bézout, il existe $u_0, v_0 \in \mathbb{Z}$ tels que

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

et on a alors

$$d = au + bv$$

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

Exercice 10 : [énoncé]
$3 \times (2n + 4) - 2 \times (3n + 3) = 6$ donc $\mathrm{pgcd}(2n + 4, 3n + 3) \mid 6$.

Exercice 11 : [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 12 : [énoncé]
Soit $(x, y) \in \mathbb{N}^2$ un couple solution. Posons $\delta = \mathrm{pgcd}(x, y)$.
On peut écrire

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

L'équation devient :

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

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 13 : [énoncé]
a) Soit (x, y) solution. $\mathrm{pgcd}(x, y) = 5$ donc $x = 5x'$ et $y = 5y'$ avec $x', y' \in \mathbb{N}$ premiers entre eux.
$\mathrm{ppcm}(x, y) = 5x'y' = 60$ 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. $\mathrm{pgcd}(x, y) = 10$ 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 14 : [énoncé]
Posons $d = \mathrm{pgcd}(a, a + b)$.
On a $d \mid a$ et $d \mid (a + b)$ alors $d \mid b = (a + b) - a$ donc $d \mid \mathrm{pgcd}(a, b) = 1$ puis $d = 1$.
De même $\mathrm{pgcd}(b, a + b) = 1$. Ainsi $a \wedge (a + b) = b \wedge (a + b) = 1$ et par suite $ab \wedge (a + b) = 1$.

Exercice 15 : [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 16 : [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 17 : [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 18 : [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 19 : [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 $a \neq 0$).
c) Inversement les couples de la forme ci-dessus sont solutions.

Exercice 20 : [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 21 : [énoncé]
Unicité : Si (d_1, d_2) est solution alors $\text{pgcd}(d, a) = \text{pgcd}(d_1d_2, a)$
Or $d_2 \wedge a = 1$ car $d_2 \mid b$ et $a \wedge b = 1$, donc $\text{pgcd}(d_1d_2, a) = \text{pgcd}(d_1, a) = d_1$ 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 $d_1d_2 \mid d$.
Inversement : Par l'égalité de Bézout on peut écrire $d_1 = u_1d + v_1a$ et $d_2 = u_2d + v_2b$ donc $d \mid d_1d_2 = Ud + v_1v_2ab$ car $d \mid ab$.

Exercice 22 : [énoncé]
Si $k \mid a$ et $\ell \mid b$ alors $k\ell \mid ab$. Ainsi $\varphi(\text{div}(a) \times \text{div}(b)) \subset \text{div}(ab)$.
Soit $d \in \text{div}(ab)$. Posons $k = \text{pgcd}(d, a)$ et $\ell = \text{pgcd}(d, b)$. On a $k \in \text{div}(a)$, $\ell \in \text{div}(b)$ et $k \wedge \ell = 1$ car $a \wedge b = 1$. Comme $k \mid d$, $\ell \mid d$ et $k \wedge \ell = 1$ on a $k\ell \mid d$. De plus $k = du + av$ et $\ell = du' + bv$ donc $k\ell = dU + abV$ d'où $d \mid k\ell$ et finalement $d = k\ell$. Ainsi $\varphi(\text{div}(a) \times \text{div}(b)) = \text{div}(ab)$.
Soit $(k, \ell) \in \text{div}(a) \times \text{div}(b)$ et $(k', \ell') \in \text{div}(a) \times \text{div}(b)$. Si $\varphi(k, \ell) = \varphi(k', \ell')$ alors $k\ell = k'\ell'$.
Comme $k \mid k'\ell'$ et $k \wedge \ell' = 1$ on a $k \mid k'$. De même $k' \mid k$ donc $k = k'$. De même $\ell = \ell'$.
Ainsi φ est injective et finalement φ réalise une bijection de $\text{div}(a) \times \text{div}(b)$ vers $\text{div}(ab)$.

Exercice 23 : [énoncé]
Par l'absurde, supposons que a_i et a_j (avec $i, j \in \{1, \ldots, n+1\}$) 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 24 : [énoncé]
Notons $2p + 1$ le premier nombre impair sommé. On a
$$N = \sum_{k=0}^{n-1}(2k + 2p + 1) = n(n + 2p)$$
avec $n \geqslant 2$ et $n + 2p \geqslant 2$. Ainsi N est composé.

Exercice 25 : [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 $n \in \mathbb{N}^\star$ car $2n + 1 \geqslant 2$ et $2n^2 + 2n + 1 \geqslant 2$.
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 $n^2 + 3\text{n} + 4 = 0{,}1$ ou -1 n'ont pas de solutions car toutes de discriminant négatif. Par conséquent $n^4 - n^2 + 16$ est composée.

Exercice 26 : [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 27 : [énoncé]
Considérons les $x_k = 1001! + k$ avec $2 \leqslant k \leqslant 1001$. Ce sont 1000 entiers consécutifs.
Pour tout $2 \leqslant k \leqslant 1001$, on a $k \mid (1001)!$ donc $k \mid x_k$ avec $2 \leqslant k < x_k$ donc $x_k \notin \mathcal{P}$.

Exercice 28 : [énoncé]
On peut factoriser
$$p^2 - 1 = (p-1)(p+1)$$
p est impair donc les nombres $p-1$ et $p+1$ sont deux entiers pairs consécutifs, l'un est divisible par 2, l'autre par 4. Ainsi
$$8 \mid p^2 - 1$$
Les entiers $p-1, p, p+1$ sont consécutifs, l'un est divisible par 3, ce ne peut être p car $p \geqslant 5$ premier. Ainsi
$$3 \mid p^2 - 1$$
Enfin, 3 et 8 étant premiers entre eux
$$24 \mid p^2 - 1$$

Exercice 29 : [énoncé]
Si $n = ab$ avec $a, b \in \mathbb{N}^\star$ 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 30 : [énoncé]
Supposons que $a^p - 1$ premier.
Comme $a^p - 1 = (a-1)(1 + a + \cdots + a^{p-1})$ on a $a - 1 = 1$ ou $1 + a + \cdots + a^{p-1} = 1$.
Or $p \geqslant 2$ et $a \neq 0$ donc $1 + a + \cdots + a^{p-1} \neq 1$. Par conséquent $a = 2$.
Montrons maintenant que p est premier.
Si $d \mid p$ alors on peut écrire $p = cd$ puis $a^p - 1 = (a^d)^c - 1$.
Si $d \neq p$ alors $c \geqslant 2$ puis par le résultat précédent on obtient $a^d = 2$ puis $d = 1$.
Ainsi les seuls diviseurs de p sont 1 et lui-même.
Finalement p est premier.

Exercice 31 : [énoncé]
On peut écrire
$$n = 2^k(2p+1)$$
On a alors
$$a^n + 1 = b^{2p+1} - (-1)^{2p+1} = (b+1)c$$
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 32 : [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 $\alpha, \beta \geqslant 1$, le cas $\alpha + \beta = 1$ est à exclure et puisque $\alpha \leqslant a^n$ et $\beta \leqslant b^n$, le cas $\alpha + \beta = a^n + b^n$ entraîne
$$\alpha = a^n \text{ et } \beta = b^n$$
Puisque $a \geqslant 2$, l'égalité $\alpha = a^n = \alpha^{2p+1}$ entraîne $p = 0$ et finalement n est une puissance de 2.

Exercice 33 : [énoncé]
a) n est impair, il n'est donc pas divisible par 2. Si tous les nombres premiers p divisant n sont tels que $p = 1 \quad [4]$ alors $n = 1 \quad [4]$ et donc $n \notin E$
b) Supposons qu'il n'y en ait qu'un nombre fini de nombres premiers $p_1 p_2 \ldots p_n$.
Considérons
$$n = 4p_1p_2 \ldots p_n - 1 \in E$$
Il existe $p \in \mathcal{P} \cap E$ tel que $p \mid n$ mais $p \mid p_1 p_2 \ldots p_n$ donc $p \mid 1$. Absurde.

Exercice 34 : [énoncé]
Par l'absurde, supposons qu'il n'y ait qu'un nombre fini de nombres premiers de la forme $4n + 3$. On peut introduire le nombre N égal au produit de ceux-ci.
Considérons alors l'entier $4N - 1$.
$4N - 1$ est impair donc 2 ne le divise pas.
Si tous les facteurs premiers de $4N - 1$ sont égaux à 1 modulo 4 alors $4N - 1 \equiv 1 \quad [4]$ ce qui est absurde.
L'un au moins des facteurs premiers de $4N - 1$ est alors de la forme $4n + 3$ et celui-ci apparaît donc dans le produit N . Ce facteur premier divise alors les nombres $4N - 1$ et N, il divise donc -1, c'est absurde !

Exercice 35 : [énoncé]
a) Quitte à échanger, supposons $n < m$.
On remarque que
$$(F_n - 1)^{2^{m-n}} = F_m - 1$$
En développant cette relation par la formule du binôme, on parvient à une relation de la forme
$$F_m + vF_n = 2$$
avec $v \in \mathbb{Z}$ car les coefficients binomiaux sont des entiers.
On en déduit que $\operatorname{pgcd}(F_n, F_m) = 1$ ou 2.
Puisque F_n et F_m ne sont pas tous deux pairs, ils sont premiers entre eux.
b) Les F_n sont en nombre infini et possèdent des facteurs premiers distincts, il existe donc une infinité de nombres premiers.

Exercice 36 : [énoncé]
($\Leftarrow$) ok
($\Rightarrow$) 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 37 : [énoncé]
Supposons $a^2 \mid b^2$.
Posons $d = \operatorname{pgcd}(a, b)$. On a $d^2 = \operatorname{pgcd}(a, b)^2 = \operatorname{pgcd}(a^2, b^2) = a^2$ donc $d = |a|$ puis $a \mid b$.

Exercice 38 : [énoncé]
On peut écrire $x = \frac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^\star$ 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 39 : [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 40 : [énoncé]
Le nombre de côté du polygone construit est le plus petit entier $k \in \mathbb{N}^\star$ tel que $n \mid kp$.
Posons $\delta = \operatorname{pgcd}(n, p)$. On peut écrire $n = \delta n'$ et $p = \delta p'$ avec $n' \wedge p' = 1$.
$n \mid kp \Leftrightarrow n' \mid kp'$ i.e. $n' \mid k$. Ainsi $k = n' = n/\delta$.

Exercice 41 : [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 42 : [énoncé]
a) Supposons $\sqrt{6} = p/q$ avec $p \wedge q = 1$. On a $6q^2 = p^2$ donc p pair, $p = 2k$. On obtient alors $3q^2 = 2k^2$ et donc q est pair. Absurde car p et q sont premiers entre eux.
b) Par développement selon la formule du binôme de Newton
$$(a + \sqrt{b})^n = \alpha_k + \beta_k \sqrt{b} \text{ avec } \alpha_k, \beta_k \in \mathbb{Z}$$
c) $a + \sqrt{b}$ racine de $P = \sum_{k=0}^{n} a_k X^k$ donne
$$\sum_{k=0}^{n} a_k \alpha_k = \left(\sum_{k=0}^{n} a_k \beta_k \right) \sqrt{b}$$
L'irrationalité de $\sqrt{b}$ entraîne
$$\sum_{k=0}^{n} a_k \alpha_k = \sum_{k=0}^{n} a_k \beta_k = 0$$
ce qui permet de justifier qu'alors $P(a - \sqrt{b}) = 0$.
d) Posons
$$Q = (X - a + \sqrt{b})(X - a - \sqrt{b}) = X^2 - 2aX + a^2 - b \in \mathbb{Z}[X]$$

Par division euclidienne $P = QS + T$ avec $\deg T < 2$. Or en posant cette division euclidienne, on peut affirmer que $S, T \in \mathbb{Z}[X]$ avec $P, Q \in \mathbb{Z}[X]$ et Q unitaire. $a + \sqrt{b}, a - \sqrt{b}$ racine de P entraîne $T = 0$ et donc $P = QS$ avec $Q, S \in \mathbb{Z}[X]$. En dérivant $P' = Q'S + QS'$ et $a + \sqrt{b}$ entraîne racine de P' donne $a + \sqrt{b}$ racine de S. On peut alors comme ci-dessus justifier $S = QR$ avec $R \in \mathbb{Z}[X]$ et conclure.

Exercice 43 : [énoncé]
On peut écrire

$$\sum_{k=1}^{n} d(k) = \sum_{k=1}^{n} \sum_{d|k} 1$$

et en permutant les deux sommes

$$\sum_{k=1}^{n} d(k) = \sum_{d=1}^{n} \sum_{k \in A_d} 1$$

avec A_d l'ensemble des multiples de d qui sont inférieurs à n. On a évidemment

$$\operatorname{Card} A_d = E(n/d)$$

et donc

$$\sum_{k=1}^{n} d(k) = \sum_{d=1}^{n} E\left(\frac{n}{d}\right)$$

Puisque

$$x - 1 < E(x) \leqslant x$$

on obtient l'encadrement

$$n\left(\sum_{d=1}^{n} \frac{1}{d} - 1\right) \leqslant \sum_{k=1}^{n} d(k) \leqslant n \sum_{d=1}^{n} \frac{1}{d}$$

Sachant qu'il est connu que

$$\sum_{k=1}^{n} \frac{1}{d} \sim \ln n$$

on obtient

$$\frac{1}{n} \sum_{k=1}^{n} d(k) \sim \ln n$$

Exercice 44 : [énoncé]
($\Leftarrow$) clair
($\Rightarrow$) n est divisible par un nombre premier p et ne peut lui être égal. On peut donc écrire $n = pd$ avec $1 < d < n$. Si d est premier alors on obtient la seconde forme. Sinon, il ne peut qu'être divisible par p (car $q \mid d$ implique que n est un multiple de pqd car n est produit de ses diviseurs non triviaux). Le nombre d est alors de la forme $d = p^k$. $k = 1$ et $k \geqslant 3$ sont à exclure puisque n est le produit de ses diviseurs non triviaux. Il reste $d = p^2$ et alors $n = p^3$

Exercice 45 : [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 $p^\beta \leqslant p^\alpha$ puis $\beta \leqslant \alpha$.
Inversement : ok.

Exercice 46 : [énoncé]
Les diviseurs positifs sont les $d = \prod_{k=1}^{N} p_k^{\beta_k}$ avec $\forall 1 \leqslant k \leqslant N, 0 \leqslant \beta_k \leqslant \alpha_k$.
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 47 : [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 $p_1, \ldots, p_N$.
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 $\beta_i \leqslant \alpha_i$.
Ainsi d est de la forme $d = \prod_{i=1}^{N} p_i^{\beta_i}$ avec pour tout $i \in \{1, \ldots, N\}$, $0 \leqslant \beta_i \leqslant \alpha_i$.
Inversement de tels nombres sont bien diviseurs de n.
Il y a autant de nombres de cette forme distincts que de choix pour les
$\beta_1, \ldots, \beta_N$.Pour β_i, il y a $\alpha_i + 1$ choix possibles, au total $d(n) = \prod_{i=1}^{N} (\alpha_i + 1)$.
De plus

$$\sigma(n) = \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \ldots \sum_{\beta_N=0}^{\alpha_N} p_1^{\beta_1} p_2^{\beta_2} \ldots p_N^{\beta_N} = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1}\right) \left(\sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2}\right) \ldots \left(\sum_{\beta_N=0}^{\alpha_N} p_N^{\beta_N}\right)$$

Par sommation géométrique

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

Exercice 48 : [énoncé]
a) $Div(p^\alpha) \cap \mathbb{N} = \left\{1, p, p^2, \dots, p^\alpha\right\}$ 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) $\sigma(ab) = \sum\limits_{d \mid ab} d = \sum\limits_{d_1 \mid a} \sum\limits_{d_2 \mid b} d_1 d_2 = \left(\sum\limits_{d_1 \mid a} d_1\right)\left(\sum\limits_{d_2 \mid b} d_b\right) = \sigma(a)\sigma(b)$.
d) Si $n = p_1^{\alpha_1} \dots p_N^{\alpha_N}$ alors $\sigma(n) = \prod\limits_{i=1}^{N} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$.

Exercice 49 : [énoncé]
Si le couple (x_0, y_0) est entier la conclusion est entendue.
Sinon, on peut écrire

$$x_0 = p_0/d_0 \text{ et } y_0 = q_0/d_0 \text{ avec } p_0, q_0 \in \mathbb{Z} \text{ et } d_0 \in \mathbb{N} \setminus \{0, 1\}$$

Considérons alors un couple entier (x_0', y_0') obtenu par arrondi de (x_0, y_0). On a

$$D^2 = (x_0 - x_0')^2 + (y_0 - y_0')^2 \leqslant 1/4 + 1/4$$

La droite joignant nos deux couples peut être paramétrée par

$$\begin{cases} x = x_0' + \lambda(x_0 - x_0') \\ y = y_0' + \lambda(y_0 - y_0') \end{cases} \text{avec } \lambda \in \mathbb{R}$$

Cette droite coupe le cercle en (x_0, y_0) pour $\lambda = 1$ et recoupe encore celui-ci en (x_1, y_1) obtenu pour

$$\lambda = \frac{(x_0')^2 + (y_0')^2 - N^2}{D^2}$$

Puisque

$$D^2 = N^2 - 2(x_0 x_0' + y_0 y_0') + (x_0')^2 + (y_0')^2 = \frac{d_1}{d_0}$$

avec $d_1 \in \mathbb{N}^\star$ et $d_1 < d_0$ car $D^2 < 1$.
Le nombre λ est donc de la forme $d_0 k/d_1$ avec k entier et les coordonnées (x_1, y_1) sont alors de la forme

$$x_1 = p_1/d_1 \text{ et } y_1 = q_1/d_1 \text{ avec } p_1, q_1 \in \mathbb{Z} \text{ et } d_1 \in \mathbb{N}^\star,\ d_1 < d_0$$

Si $d_1 = 1$, le processus s'arrête, sinon il suffit de répéter l'opération jusqu'à obtention d'un couple entier.

Exercice 50 : [énoncé]
a) $v_2(1000!) = 500 + v_2(500!)$ car $1000! = 2^{500} \times 500! \times k$ avec k produit de nombres impairs.
$v_2(1000!) = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994$.
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 51 : [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. $n! = 1 \times 2 \times \ldots \times n$, 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

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

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

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

car toutes les puissances de nombres premiers intervenant dans la décomposition de $\binom{2n}{n}$ divisent $\prod_{p \in \mathcal{P}; p \leqslant 2n} p^{\left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor}$.

Notons qu'en fait ce produit désigne

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

c) On a

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

d) En passant au logarithme :

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

A l'aide d'une comparaison intégrale on obtient

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

donc

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

donc

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

Par suite

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

puis

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

On en déduit

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

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 52 : [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 $n \in \{0, 1, \dots, p-1\}$
Pour $n = 0$: ok
Supposons la propriété établie au rang $n \in \{0, 1, \dots, p-2\}$
Par la formule du binôme

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

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

$$\binom{p}{k} \equiv 0 \quad [p]$$

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

$$n^p \equiv r^p \equiv r \equiv n \quad [p]$$

Exercice 53 : [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 54 : [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.

Exercice 55 : [énoncé]
a) Puisque q divise N, on a

$$(2p_1 \dots p_r)^2 \equiv -1 \quad [q]$$

On peut écrire le nombre premier q sous la forme $4n + 3$ et alors

$$(2p_1 \dots p_r)^{(q-1)} \equiv \left[(2p_1 \dots p_r)^2\right]^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \quad [q]$$

b) Par le petit théorème de Fermat, on a aussi

$$(2p_1 \dots p_r)^{(q-1)} \equiv 1 \quad [q]$$

et puisque 1 et -1 ne sont pas congrus modulo q, on obtient une absurdité.
La décomposition en facteurs premiers de N, ne fait donc intervenir aucun nombre premier de la forme $4n + 3$. Les facteurs premiers de N ne peuvent donc qu'être 2 et ceux de la forme $4n + 1$. Ceux-ci divisent alors $2p_1 \dots p_r$ et donc, par opérations, ils divisent aussi 1.
C'est absurde.
Notons qu'on peut démontrer, plus simplement, qu'il existe aussi une infinité de nombres premiers de la forme $4n + 3$.