

# Arithmétique dans $\mathbb{Z}$

## 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 [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  $b^{n+1}$ .

## Calcul en congruence

### Exercice 4 [01190] [\[correction\]](#)

Montrer que  $11 \mid 2^{123} + 3^{121}$ .

### Exercice 5 [01191] [\[correction\]](#)

Quel est le reste de la division euclidienne de  $1234^{4321} + 4321^{1234}$  par 7 ?

### Exercice 6 [01192] [\[correction\]](#)

Montrer que pour tout  $n \in \mathbb{N}$  :

$$\begin{array}{lll} \text{a) } 6 \mid 5n^3 + n & \text{b) } 7 \mid 3^{2n+1} + 2^{n+2} & \text{c) } 5 \mid 2^{2n+1} + 3^{2n+1} \\ \text{d) } 11 \mid 3^{8n} \times 5^4 + 5^{6n} \times 7^3 & \text{e) } 9 \mid 4^n - 1 - 3n & \text{f) } 15^2 \mid 16^n - 1 - 15n \end{array}$$

### Exercice 7 [01193] [\[correction\]](#)

Trouver les entiers  $n \in \mathbb{Z}$  tel que  $10 \mid n^2 + (n+1)^2 + (n+3)^2$ .

### Exercice 8 [01194] [\[correction\]](#)

Montrer

$$7 \mid x \text{ et } 7 \mid y \Leftrightarrow 7 \mid x^2 + y^2$$

### Exercice 9 [03679] [\[correction\]](#)

Montrer que si  $n$  est entier impair alors

$$n^2 \equiv 1 \pmod{8}$$

### Exercice 10 [03680] [\[correction\]](#)

Soient  $\lambda, a, b \in \mathbb{Z}$  et  $m \in \mathbb{N}^*$ . On suppose  $\lambda$  et  $m$  premiers entre eux. Montrer

$$a \equiv b \pmod{m} \Leftrightarrow \lambda a \equiv \lambda b \pmod{m}$$

## PGCD et PPCM

### Exercice 11 [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 12 [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 13 [01197] [\[correction\]](#)

Montrer que le pgcd de  $2n + 4$  et  $3n + 3$  ne peut être que 1, 2, 3 ou 6.

### Exercice 14 [01198] [\[correction\]](#)

a) Montrer que si  $r$  est le reste de la division euclidienne de  $a \in \mathbb{N}$  par  $b \in \mathbb{N}^*$  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 15** [ 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 16** [ 01200 ] [correction]

Résoudre dans  $\mathbb{N}^2$  l'équation :

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

**Exercice 17** [ 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 18** [ 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 19** [ 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 20** [ 01204 ] [correction]

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

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

**Exercice 21** [ 01205 ] [correction]

Montrer que pour tout entier  $n \in \mathbb{N}^*$ ,  $n + 1$  et  $2n + 1$  sont premiers entre eux.

En déduire que  $n + 1 \mid \binom{2n}{n}$ .

**Exercice 22** [ 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 23** [ 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 24** [ 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 25** [ 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 26** [ 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  $\varphi : \text{div}(a) \times \text{div}(b) \rightarrow \mathbb{N}$  définie par

$$\varphi(k, \ell) = k\ell.$$

Montrer que  $\varphi$  réalise une bijection de  $\text{div}(a) \times \text{div}(b)$  vers  $\text{div}(ab)$ .

**Exercice 27** [ 01211 ] [\[correction\]](#)

Soient  $a$  et  $b$  deux entiers relatifs tels que  $a^2 \mid b^2$ . Montrer que  $a \mid b$ .

**Exercice 28** [ 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 29** [ 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 30** [ 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 31** [ 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

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

**Exercice 32** [ 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.

**Exercice 33** [ 03669 ] [\[correction\]](#)

On étudie l'équation algébrique

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

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

## Systèmes chinois

**Exercice 34** [ 01216 ] [\[correction\]](#)

Résoudre le système :

$$\begin{cases} x = 2 & [10] \\ x = 5 & [13] \end{cases}$$

**Exercice 35** [ 01217 ] [\[correction\]](#)

Soient  $a, b, a', b' \in \mathbb{Z}$  avec  $b$  et  $b'$  premiers entre eux.

Montrer que le système

$$\begin{cases} x = a & [b] \\ x = a' & [b'] \end{cases}$$

possède des solutions et que celles-ci sont congrues entre elles modulo  $bb'$ .

**Exercice 36** [ 01218 ] [\[correction\]](#)

Une bande de 17 pirates dispose d'un butin composé de  $N$  pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces. Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces. Dans un naufrage ultérieur, seul le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces. Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

## Nombres premiers et décomposition primaire

### Exercice 37 [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 38 [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 39 [03623] [correction]

Soit  $n$  un naturel non nul. Montrer qu'il existe toujours un nombre premier strictement compris entre  $n$  et  $n! + 2$ .

### Exercice 40 [01222] [correction]

Soit  $p$  un nombre premier.

- a) Montrer

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

- b) En déduire que

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

Ce dernier résultat est connu sous le nom de petit théorème de Fermat (1601-1665)

### Exercice 41 [01223] [correction]

Soit  $E = \{4k - 1/k \in \mathbb{N}^*\}$ .

- 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  $p = -1 \pmod{4}$ .

### Exercice 42 [01224] [correction]

Justifier l'existence de 1000 entiers consécutifs sans nombres premiers.

### Exercice 43 [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 44 [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

$$\forall x \in \mathbb{R}, E\left(\frac{E(px)}{p}\right) = E(x)$$

### Exercice 45 [01227] [correction]

Soit  $n \in \mathbb{N} \setminus \{0, 1\}$ . 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 46 [01228] [correction]

Soient  $p \in \mathcal{P}$  et  $\alpha \in \mathbb{N}^*$ . Déterminer les diviseurs positifs de  $p^\alpha$ .

### Exercice 47 [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 48 [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 49 [01231] [correction]

Soit  $\sigma : \mathbb{Z} \rightarrow \mathbb{N}$  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  $n$ .

**Exercice 50** Mines-Ponts MP [ 02653 ] [[correction](#)]

Soit  $p$  un nombre premier,  $p \geq 5$ . Montrer que  $p^2 - 1$  est divisible par 24.

**Exercice 51** [ 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 52** X PC [ 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.

## Corrections

### Exercice 1 : [énoncé]

a)  $x = 1$  n'est pas solution. Pour  $x \neq 1$  :

$$x - 1 \mid x + 3 \Leftrightarrow \frac{x+3}{x-1} = 1 + \frac{4}{x-1} \in \mathbb{Z} \Leftrightarrow x - 1 \in \text{Div}(4) = \{1, 2, 4, -1, -2, -4\}$$

Ainsi  $\mathcal{S} = \{2, 3, 5, 0, -1, -3\}$ .

b)  $x = -2$  n'est pas solution. Pour  $x \neq -2$  :

$$x + 2 \mid x^2 + 2 \Leftrightarrow \frac{x^2+2}{x+2} = x - 2 + \frac{6}{x+2} \in \mathbb{Z} \Leftrightarrow x + 2 \in \text{Div}(6) = \{1, 2, 3, 6, -1, -2, -3, -6\}.$$

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

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

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

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

on obtient

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

### Exercice 3 : [énoncé]

$a - 1 = bq + r$  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 4 : [énoncé]

$$2^5 = -1 \quad [11] \text{ donc } 2^{10} = 1 \quad [11] \text{ puis}$$

$$2^{123} = 2^{120} \times 2^3 = (2^{10})^{12} \times 8 = 1 \times 8 = 8 \quad [11].$$

$$3^5 = 1 \quad [11] \text{ donc } 3^{121} = 3^{120} \times 3 = (3^5)^{24} \times 3 = 1 \times 3 = 3 \quad [11].$$

$$\text{Ainsi } 2^{123} + 3^{121} = 8 + 3 = 11 \quad [11] \text{ et donc } 11 \mid 2^{123} + 3^{121}.$$

### Exercice 5 : [énoncé]

$$1234 = 2 \quad [7] \text{ et } 2^3 = 1 \quad [7] \text{ donc } 1234^{4321} = 2^{4321} = 2^{4320} \times 2 = 1 \times 2 = 2 \quad [7].$$

$$4321 = 2 \quad [7] \text{ donc } 4321^{1234} = 2^{1234} = 2^{1233} \times 2 = 1 \times 2 = 2 \quad [7].$$

$$\text{Par suite } 1234^{4321} + 4321^{1234} = 2 + 2 = 4 \quad [7]. \text{ Le reste cherché est } 4.$$

### Exercice 6 : [énoncé]

$$\text{a) Pour } n = 0, 1, 2, 3, 4, 5 \text{ on a } n^3 = n \quad [6] \text{ donc } 5n^3 + n = 6n = 0 \quad [6].$$

$$\text{b) } 3^{2n+1} + 2^{n+2} = 3 \cdot (3^2)^n + 4 \cdot 2^n = 3 \cdot 2^n + 4 \cdot 2^n = 7 \cdot 2^n = 0 \quad [7].$$

$$\text{c) } 2^{2n+1} + 3^{2n+1} = 2 \cdot (2^2)^n + 3 \cdot (3^2)^n = 2 \cdot 4^n + 3 \cdot 4^n = 5 \cdot 4^n = 0 \quad [5].$$

$$\text{d) } 3^{8n} \times 5^4 + 5^{6n} \times 7^3 = 5^n \times 9 + 5^n \times 2 = 11 \times 5^n = 0 \quad [11].$$

$$\text{e) } 4^n - 1 - 3n = (4 - 1)(1 + 4 + \dots + 4^{n-1}) - 3n = 3(1 + 4 + \dots + 4^{n-1} - n) \\ \text{or } 1 + 4 + \dots + 4^{n-1} - n = 1 + \dots + 1 - n = n - n = 0 \quad [3] \text{ donc } 9 \mid 4^n - 1 - 3n.$$

f)

$$16^n - 1 - 15n = (16 - 1)(1 + 16 + \dots + 16^{n-1}) - 15n = 15(1 + 16 + \dots + 16^{n-1} - n) \\ \text{or } 1 + 16 + \dots + 16^{n-1} - n = 1 + \dots + 1 - n = n - n = 0 \quad [15] \text{ donc}$$

$$15^2 \mid 16^n - 1 - 15n.$$

### Exercice 7 : [énoncé]

$n$	0	1	2	3	4	5	6	7	8	9
$n^2 + (n+1)^2 + (n+3)^2$	0	1	8	1	0	5	6	3	6	5

$$\text{donc } 10 \mid n^2 + (n+1)^2 + (n+3)^2 \Leftrightarrow n = 0 \text{ ou } 4 \quad [10].$$

**Exercice 8 :** [énoncé]

(⇒) ok

(⇐) On observe que :

$x$	0	1	2	3	4	5	6
$x^2$	0	1	4	2	2	4	1

modulo 7.

La seule possibilité pour que  $x^2 + y^2 = 0 [7]$  est que  $x = y = 0 [7]$ .**Exercice 9 :** [énoncé]On peut écrire  $n = 2p + 1$  et alors

$$n^2 = (2p + 1)^2 = 4p(p + 1) + 1$$

Puisque l'un des facteurs de  $p(p + 1)$  est pair, le produit  $4p(p + 1)$  est multiple de 8 et donc

$$4p(p + 1) + 1 \equiv 1 \quad [8]$$

**Exercice 10 :** [énoncé](⇒) Si  $a \equiv b \quad [m]$  alors  $m$  divise  $b - a$  et divise a fortiori  $\lambda b - \lambda a = \lambda(b - a)$ .(⇐) Si  $\lambda a \equiv \lambda b \quad [m]$  alors  $m$  divise  $\lambda(b - a)$ . Or  $m$  et  $\lambda$  sont supposés premiers entre eux donc  $m$  divise  $b - a$ .**Exercice 11 :** [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 12 :** [énoncé](⇒) Supposons  $d = au + bv$  avec  $u, v \in \mathbb{Z}$ . $\text{pgcd}(a, b) \mid a$  et  $\text{pgcd}(a, b) \mid b$  donc  $\text{pgcd}(a, b) \mid au + bv = d$ .(⇐) 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 13 :** [énoncé] $3 \times (2n + 4) - 2 \times (3n + 3) = 6$  donc  $\text{pgcd}(2n + 4, 3n + 3) \mid 6$ .**Exercice 14 :** [énoncé]a) On  $aa = bq + r$  avec  $0 \leq r < b$ .

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

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

On a

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

**Exercice 15 :** [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 16 :** [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 :

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

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 17 :** [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.

$$x + y = 10(x' + y') = 100 \text{ donc } x' + y' = 10.$$

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 18 : [énoncé]

Posons  $d = \text{pgcd}(a, a + b)$ .

On a  $d \mid a$  et  $d \mid (a + b)$  alors  $d \mid b = (a + b) - a$  donc  $d \mid \text{pgcd}(a, b) = 1$  puis  $d = 1$ .

De même  $\text{pgcd}(b, a + b) = 1$ . Ainsi  $a \wedge (a + b) = b \wedge (a + b) = 1$  et par suite  $ab \wedge (a + b) = 1$ .

### Exercice 19 : [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 20 : [énoncé]

a)  $n^2 + n = n(n + 1)$ .

$$1 \times (2n + 1) - 2 \times n = 1 \text{ donc } (2n + 1) \wedge n = 1.$$

$$2 \times (n + 1) - 1 \times (2n + 1) = 1 \text{ donc } (2n + 1) \wedge (n + 1) = 1$$

Par produit  $(2n + 1) \wedge (n^2 + n) = 1$ .

b)  $3n^2 + 2n = n(3n + 2)$ .

$$1 \times (n + 1) - 1 \times n = 1 \text{ donc } n \wedge (n + 1) = 1.$$

$$3 \times (n + 1) - 1 \times (3n + 2) = 1 \text{ donc } (3n + 2) \wedge (n + 1) = 1.$$

Par produit  $(3n^2 + 2n) \wedge (n + 1) = 1$ .

### Exercice 21 : [énoncé]

$$2 \times (n + 1) - 1 \times (2n + 1) = 1 \text{ donc } (n + 1) \wedge (2n + 1) = 1.$$

$$\binom{2n+1}{n+1} = \frac{2n+1}{n+1} \binom{2n}{n} \text{ donc } (n+1) \binom{2n+1}{n+1} = (2n+1) \binom{2n}{n}.$$

Puisque  $\binom{2n+1}{n+1} \in \mathbb{Z}$ , on a  $(n + 1) \mid (2n + 1) \binom{2n}{n}$  or  $(n + 1) \wedge (2n + 1) = 1$

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

### Exercice 22 : [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 23 : [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 24 : [énoncé]

a) Unicité : Si  $(a_n, b_n)$  et  $(\alpha_n, \beta_n)$  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

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

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

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



b) On a

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

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 25 : [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  $d \mid d_1 d_2 = U d + v_1 v_2 a b$  car  $d \mid ab$ .

### Exercice 26 : [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  $\varphi$  est injective et finalement  $\varphi$  réalise une bijection de  $\text{div}(a) \times \text{div}(b)$  vers  $\text{div}(ab)$ .

### Exercice 27 : [énoncé]

Supposons  $a^2 \mid b^2$ .

Posons  $d = \text{pgcd}(a, b)$ . On a  $d^2 = \text{pgcd}(a, b)^2 = \text{pgcd}(a^2, b^2) = a^2$  donc  $d = |a|$  puis  $a \mid b$ .

### Exercice 28 : [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 29 : [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 30 : [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  $n' \wedge p' = 1$ .

$n \mid kp \Leftrightarrow n' \mid kp'$  i.e.  $n' \mid k$ . Ainsi  $k = n' = n/\delta$ .

### Exercice 31 : [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  $n \geq 1$ .

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

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  $m \in \mathbb{N}^*$

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  $n \geq 1$

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

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  $\text{pgcd}(m, n)$  :

$$a_0 = m, a_1 = n, a_0 = a_1 q_1 + a_2, a_1 = a_2 q_2 + a_3, \dots, a_{p-1} = a_p q_p + 0 \text{ avec}$$

$$a_p = \text{pgcd}(m, n)$$

$$\text{Or } \text{pgcd}(\varphi_n, \varphi_m) = \text{pgcd}(\varphi_{a_0}, \varphi_{a_1}) = \text{pgcd}(\varphi_{a_1}, \varphi_{a_2}) = \dots = \text{pgcd}(\varphi_{a_p}, \varphi_0) = \varphi_{a_p}$$

car  $\varphi_0 = 0$ .

$$\text{Ainsi } \text{pgcd}(\varphi_m, \varphi_n) = \varphi_{\text{pgcd}(m, n)}.$$

### Exercice 32 : [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  $(i - j) \cdot n!$ .

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  $a_i = i \cdot n! + 1$  et donc  $d$  divise 1.

C'est absurde.

### Exercice 33 : [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

$$p^n + a_{n-1}qp^{n-1} + \dots + a_1pq^{n-1} + a_0q^n = 0$$

Puisque  $q$  divise  $a_{n-1}qp^{n-1} + \dots + a_1pq^{n-1} + a_0q^n$ , 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 34 : [énoncé]

Déterminons une solution particulière :  $x = 2 + 10k = 5 + 13k'$  avec  $k, k' \in \mathbb{Z}$ .  $10k - 13k' = 3$ . Cherchons  $u, v \in \mathbb{Z}$  tel que  $10u + 13v = 1$ .  $u = 4$  et  $v = -3$  conviennent.

Prenons  $k = 12$ ,  $k' = 9$  ce qui donne  $x = 122$ .

Soit  $x$  une autre solution. On a

$$\begin{cases} x = 122 & [10] \\ x = 122 & [13] \end{cases}$$

donc  $10 \mid x - 122$  et  $13 \mid x - 122$  donc  $130 \mid x - 122$  et par suite  $x = 122 + 130k$  avec  $k \in \mathbb{Z}$ .

Inversement : ok.

### Exercice 35 : [énoncé]

Il existe  $u, v \in \mathbb{Z}$  tel que  $bu + b'v = 1$ .

Soit  $x = a'bu + ab'v$ .

On a  $x = a'bu + a - abu = a \quad [b]$  et  $x = a' - a'b'v + ab'v = a' \quad [b']$  donc  $x$  est solution.

Soit  $x'$  une autre solution. On a  $x = x' \quad [b]$  et  $x = x' \quad [b']$  donc  $b \mid (x' - x)$  et  $b' \mid (x' - x)$ .

Or  $b \wedge b' = 1$  donc  $bb' \mid (x' - x)$ .

Inversement, soit  $x'$  tel que  $bb' \mid x' - x$ , on a bien  $x' = x = a \quad [b]$  et  $x' = x = a' \quad [b']$ .

### Exercice 36 : [énoncé]

Notons  $x \in \mathbb{N}$  le montant du trésor. De part les hypothèses

$$\begin{cases} x = 3 & [17] \\ x = 4 & [11] \\ x = 5 & [6] \end{cases}$$

Déterminons un entier  $x$  tel que  $x = 3 + 17k = 4 + 11k' = 5 + 6k''$  avec  $k, k', k'' \in \mathbb{Z}$ .

$$\text{On a } \begin{cases} 11k' - 6k'' = 1 \\ 17k - 11k' = 1 \end{cases} \text{ donc } 17k - 6k'' = 2.$$

Or  $k = -2$  et  $k'' = -6$  définit une solution particulière de cette équation dont la solution générale est alors

$$k = -2 + 6\ell \text{ et } k'' = -6 + 17\ell \text{ car } 6 \wedge 17 = 1$$

Prenons  $\ell$  de sorte que  $11 \mid 17k - 1$ .

$$17k - 1 = -35 + 102\ell = -2 + 3\ell \quad [11]$$

Pour  $\ell = 8$ ,  $k = 46$ ,  $k' = 71$  et  $k'' = 130$  on a  $x = 785$ .

La solution générale du système est

$$x = 785 + 1122k$$

### Exercice 37 : [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 38 : [énoncé]

Supposons que  $a^p - 1$  premier.

Comme  $a^p - 1 = (a-1)(1+a+\dots+a^{p-1})$  on a  $a-1 = 1$  ou

$$1+a+\dots+a^{p-1} = 1.$$

Or  $p \geq 2$  et  $a \neq 0$  donc  $1+a+\dots+a^{p-1} \neq 1$ . 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  $c \geq 2$  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 39 : [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 40 : [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  $1 \leq k \leq p-1$ .

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

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 41 : [énoncé]

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

b) Supposons qu'il n'y en ait qu'un nombre fini de nombres premiers  $p_1 p_2 \dots p_n$ . 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 42 :** [énoncé]

Considérons les  $x_k = 1001! + k$  avec  $2 \leq k \leq 1001$ . Ce sont 1000 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 43 :** [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 44 :** [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)

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

or

$$E\left(\frac{E(px)}{p}\right) = E(x)$$

avec  $x = \frac{n}{p^2}$  donne

$$E\left(\frac{E(n/p)}{p}\right) = E\left(\frac{n}{p^2}\right)$$

puis finalement

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

avec

$$k = E\left(\frac{\ln n}{\ln p}\right)$$

**Exercice 45 :** [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  $k \geq 3$  sont à exclure puisque  $n$  est le produit de ses diviseurs non triviaux. Il reste  $d = p^2$  et alors  $n = p^3$

**Exercice 46 :** [énoncé]

Soit  $d \in \text{Div}(p^\alpha) \cap \mathbb{N}$ . Notons  $\beta$  la plus grande puissance de  $p$  telle que  $p^\beta \mid d$ .

On peut écrire  $d = p^\beta k$  avec  $p \nmid k$ .

Puisque  $p \nmid k$  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 47 :** [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  $\beta_k$  conduisant à des diviseurs distincts, il y a exactement

$$\prod_{k=1}^N (\alpha_k + 1) \text{ diviseurs positifs de } n.$$

**Exercice 48 :** [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  $\beta_i$ , il y a  $\alpha_i + 1$  choix possibles, au total  $d(n) = \prod_{i=1}^N (\alpha_i + 1)$ .

De plus

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

Par sommation géométrique

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

**Exercice 49 :** [énoncé]

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

b) Soit  $d \in \text{Div}(ab) \cap \mathbb{N}$ . Posons  $d_1 = \text{pgcd}(d, a)$  et  $d_2 = \text{pgcd}(d, b)$ .

On a  $d_1 \in \text{Div}(a) \cap \mathbb{N}$  et  $d_2 \in \text{Div}(b) \cap \mathbb{N}$ .

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  $\delta_1 \in \text{Div}(a) \cap \mathbb{N}$  et  $\delta_2 \in \text{Div}(b) \cap \mathbb{N}$ .

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  $d_2 = \delta_2$ .

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

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

**Exercice 50 :** [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  $p \geq 5$  premier. Ainsi

$$3 \mid p^2 - 1$$

Enfin, 3 et 8 étant premiers entre eux

$$24 \mid p^2 - 1$$

**Exercice 51 :** [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 52 :** [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

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

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  $\alpha = a^n = \alpha^{2^{p+1}}$  entraîne  $p = 0$  et finalement  $n$  est une puissance de 2.