
Feuille d'exercices n° 8
ARITHMÉTIQUE

Exercice 1. Effectuer la division euclidienne de a par b pour les valeurs de a et b suivantes :

a) $a = 2867$ et $b = 6$;

b) $a = 7813$ et $b = -12$;

c) $a = -959$ et $b = 6$;

d) $a = -1733$ et $b = -5$.

Solution

a) $2867 = 6 * 477 + 5$;

b) $7813 = (-651) * (-12) + 1$;

c) $-959 = 6 * (-160) + 1$;

d) $-1733 = (-5) * 347 + 2$.

Exercice 2. Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$.

1. Montrer que si b divise a, alors $2^b - 1$ divise $2^a - 1$.
2. On note r le reste de la division euclidienne de a par b. Montrer que $2^r - 1$ est le reste de la division euclidienne de $2^a - 1$ par $2^b - 1$.

Solution

1. Il y a plusieurs solutions, on peut entre autre reconnaître la formule $x^n - 1 = (x - 1) * (x^{n-1} + x^{n-2} + \cdots + 1)$. On peut aussi faire ainsi (le cas $a = 0$ est évident, donc on suppose $a \geq b$) :

$$2^a - 1 = 2^a - 2^b + 2^b - 1 = 2^b(2^{a-b} - 1) + 2^b - 1.$$

On reconnaît alors en $a - b$ un multiple de b ; de plus, si $2^{a-b} - 1 = p * (2^b - 1)$ on a alors $2^a - 1 = (2^b - 1)(2^b p + 1)$. Cela signifie qu'on peut effectuer une récurrence dont la rédaction est laissée au lecteur.

2. On a $2^a - 1 - (2^r - 1) = 2^a - 2^r = 2^r(2^{a-r} - 1) = 2^r(p(2^b - 1))$ en utilisant la question 1. Comme de plus $2^r - 1 < 2^b - 1$ on a bien le résultat annoncé.

Exercice 3. Montrer qu'il n'existe pas de couple $(a, b) \in \mathbb{Z}^2$ tel que $7a - 4b^3 = 1$. *(Indication : raisonner modulo 7).*

Solution

$(7a - 4b^3 = 1) \Rightarrow (4b^3 \equiv 6 \pmod 7)$. Il suffit dès lors de rechercher les différentes valeurs atteintes : $4*1^3 \equiv 4 \pmod 7$; $4 * 2^3 \equiv 4 \pmod 7$; $4 * 3^3 \equiv 3 \pmod 7$; $4 * 4^3 \equiv 4 \pmod 7$; $4 * 5^3 \equiv 3 \pmod 7$; $4 * 6^3 \equiv 3 \pmod 7$. On constate que 1 n'est jamais atteint.

Exercice 4.

1. (a) Déterminer $k_0 \in \mathbb{N}^*$ tel que $7^{k_0} \equiv 1\ [12]$.
   (b) Déterminer $k_1 \in \mathbb{N}^*$ tel que $6^{k_0} \equiv 0\ [12]$.
   (c) Déterminer $(k_2, k_3) \in \mathbb{N}^2$ tel que $k_2 < k_3$ et $3^{k_2} \equiv 3^{k_3}\ [12]$.
   (d) Déterminer les restes de la division euclidienne par 12 des nombres suivants : 7^{30}, 6^{13}, 3^{17}, 31^{77}, $19^5 + 30^{144} + 15^{10}$.
2. Démontrer que $2^{123} + 3^{121}$ est divisible par 11.
3. Déterminer le reste de la division euclidienne de 122^{137} par 9.

Solution

1. (a) $7^2 = 49 = 48 + 1 \equiv 1\ [12]$
   (b) $6^2 = 12 * 3 \equiv 0\ [12]$
   (c) $3^3 = 27 = 24 + 3 \equiv 3^1\ [12]$
   (d) $7^30 = (7^2)^{15} \equiv 1^{15}\ [12] \equiv 1\ [12]$;
   $6^{13} = 6^2 * 6^{11} \equiv 0\ [12]$;
   $3^{17} = 3^2 * (3^3)^5 \equiv 3^{5+2}\ [12] \equiv 3^{6+1}\ [12] \equiv 3^3\ [12] \equiv 3\ [12]$.
   On a $31 \equiv 7\ [12]$ d'où $31^{77} \equiv 7^{77}\ [12] \equiv (7^2)^{38} * 7\ [12] \equiv 7\ [12]$.
   Comme $19 \equiv 7\ [12]$ et $30 \equiv 6\ [12]$ et $15 \equiv 3\ [12]$ on trouve : $19^5 + 30^{144} + 15^{10} \equiv 7+0+9\ [12] \equiv 4\ [12]$.
2. Par calcul successifs de congruence, on obtient $3^{10} \equiv 2^{10}\ [11] \equiv 1\ [11]$ (c'est un fait un résultat connu de manière plus générale, pour b premier et a non multiple de b on a toujours $a^{b-1} \equiv 1\ [b]$). Alors $2^{123} + 3^{121} \equiv 2^3 + 3\ [11] \equiv 11\ [11]$.
3. On calcule $122 \equiv 5\ [9]$. Ensuite, en calculant les puissances successives de 5 modulo 9 on obtient $5^6 \equiv 1\ [9]$ et on cherche $137 \pmod 6$. On trouve alors $122^{137} \equiv 5^5\ [9] \equiv 2\ [9]$.

Exercice 5. Déterminer le dernier chiffre de l'écriture décimale de 3^{1111}.

Solution

Ce que l'on cherche ici, c'est le reste modulo 10. On trouve $3^4 \equiv 1\ [10]$. On cherche alors 1111 mod (4). On a $1111 \equiv 11\ [4] \equiv 3\ [4]$, d'où le dernier chiffre cherché est 7.

Exercice 6.

1. Calculer le plus grand diviseur commun de 126 et 230.
2. Soit $(a, b, c) \in \mathbb{Z}^3$. Soit $n \in \mathbb{Z}$. Montrer que n divise a, b et c si, et seulement si, il divise $\operatorname{pgcd}(a, b)$ et c. En déduire que
$$\operatorname{pgcd}(\operatorname{pgcd}(a, b), c) = \operatorname{pgcd}(a, \operatorname{pgcd}(b, c)).$$
   On définit alors $\operatorname{pgcd}(a, b, c) = \operatorname{pgcd}(\operatorname{pgcd}(a, b), c)$.
3. Calculer le plus grand diviseur commun des triples d'entiers suivants :
   a) $(390, 720, 450)$; b) $(180, 606, 750)$.

Solution

1. On a $126 = 2 \cdot 3^2 \cdot 7$ et $230 = 2 \cdot 115 = 2 \cdot 5 \cdot 23$ donc le pgcd est 2.
2. Soit $n \in \mathbb{Z}$ avec $n |\operatorname{pgcd}(a, b)$ et c. Alors $n|a$ et b (car $\operatorname{pgcd}(a, b)|a$ et b), et c. Si maintenant $n|a$ et b, $n|\operatorname{pgcd}(a, b)$ d'où le résultat annoncé. Les diviseurs de a, b et c sont donc les diviseurs de $\operatorname{pgcd}(a, b)$ et c ainsi que ceux de $\operatorname{pgcd}(c, b)$ et a par symétrie des rôles. Prendre leur sup donne donc les deux pgcd proposés.
3. a) $390 = 2 \cdot 3 \cdot 5 \cdot 13$; $720 = 2^4 \cdot 3^2 \cdot 5$; $450 = 2 \cdot 3^2 \cdot 5^2$ donc le pgcd est $2 \cdot 3 \cdot 5 = 30$.

   b) Ici de la même façon on trouve 6.

Exercice 7. Déterminer les couples d'entiers naturels (m, n) tels que

a) $\mathrm{pgcd}(m, n) = 18$ et $m + n = 360$; b) $\mathrm{pgcd}(m, n) = 18$ et $mn = 6480$.

Solution

a)

$$(\mathrm{pgcd}(m, n) = 18 \text{ et } m + n = 360)$$

$$\Leftrightarrow (m = 18m' \text{ et } n = 18n' \text{ et } \mathrm{pgcd}(m', n') = 1 \text{ et } m' + n' = \frac{360}{18} = 20).$$

On cherche les couples d'entiers naturels satisfaisant ces conditions. On trouve $(19, 1)$; $(17, 3)$; $(13, 7)$; $(11, 9)$ et leur symétrique, donc les solutions sont les couples

$$(19 * 18, 18);\ (17 * 18, 3 * 18);\ (13 * 18, 7 * 18);\ (11 * 18, 9 * 18)$$

et leur symétrique.

b) $\mathrm{pgcd}(m, n) = 18$ et $mn = 6480$

$$\Leftrightarrow m = 18m' \text{ et } n = 18n' \text{ et } \mathrm{pgcd}(m', n') = 1 \text{ et } m'n' = \frac{6480}{18^2}$$

. On a

$$6480 = 2 * 5 * 648 = 2^2 * 5 * 324 = 2^3 * 5 * 162 = 2^4 * 5 * 81 = 2^4 * 5 * 3^4 = 18^2 * 2^2 * 5.$$

Donc $m'n' = 2^2 * 5$. Les couples solutions sont donc $(18 * 20, 18)$ et $(18 * 2^2, 18 * 5)$ ainsi que leur symétrique.

Exercice 8. Soit $(a, b) \in \mathbb{Z}^2$.

1. Montrer que si $\mathrm{pgcd}(a, b) = 1$, alors pour tout $(p, q) \in \mathbb{Z}^2$, on a l'équivalence : $ap = bq$ si, et seulement si, il existe $k \in \mathbb{Z}$ tel que $p = bk$ et $q = ak$.
2. Étudier la réciproque.

Solution

1. Soient k, p, q entiers tels que $ka = q$ et $kb = p$. Alors

$$ap = akb = qb.$$

   Supposons maintenant que $\mathrm{pgcd}(a, b) = 1$ et que p et q sont tels que $ap = bq$. Alors via Bézout, puisque $a|bq$ on a $\exists k \in \mathbb{Z}$ tel que $q = ak$. Donc $ap = bka$ d'où $p = bk$. Pour obtenir ce résultat, si a est non nul, on divise par a ; si a est nul, $b = 1$ ou $b = -1$ nécessairement, et $q = 0$, donc on peut choisir $k = p$ initialement et le tour est bouclé.

   Donc, si $\mathrm{pgcd}(a, b) = 1$, on a bien pour tout $(p, q) \in \mathbb{Z}^2$ l'équivalence : $ap = bq$ si, et seulement si, il existe $k \in \mathbb{Z}$ tel que $p = bk$ et $q = ak$.
2. Si $d = \mathrm{pgcd}(a, b) \neq 1$, on considère $p = \frac{b}{d}$ et $q = \frac{a}{d}$, on a alors $ap = bq$ ce qui montre que la réciproque est aussi vraie.

Exercice 9. Trouver les couples $(a, b) \in \mathbb{Z}$ solutions des équations suivantes :

a) $18a + 5b = 11$; b) $39a - 12b = 121$; c) $14a - 21b = 49$.

Solution

a) On commence par chercher pgcd$(18, 5)$; on a $1 = 2 * 18 - 6 * 5$ et donc $11 = 22 * 18 - 66 * 5$. Notre équation devient alors :

$$18a + 5b = 11$$
$$\Leftrightarrow 5(b + 66) = 18(22 - a).$$

En utilisant les résultats de l'exercice précédent, puisque pgcd$(18, 5) = 1$, on déduit que les solutions sont donc

$$\{(a, b) | \exists k \in \mathbb{Z}, b + 66 = k * 18 \text{ et } 22 - a = 5k\}$$
$$= \{(22 - 5k, 18k - 66) | k \in \mathbb{Z}\}.$$

b) Puisque $3|\ 39$ et $3|12$ il divise toute combinaison entière des deux, mais 3 ne divise pas 121, donc il n'y a pas de solution entière à ce système.

c) $14a - 21b = 49 \Leftrightarrow 2a - 3b = 7$. On procède alors comme pour la première question :

$$(2a - 3b = 7) \Leftrightarrow (\exists k \in \mathbb{Z},\ a + 7 = 3k \text{ et } b + 7 = 2k).$$

L'ensemble des solutions est donc :

$$\{(3k - 7, 2k - 7) | k \in \mathbb{Z}\}.$$

Exercice 10. Déterminer les solutions $n \in \mathbb{Z}$ des systèmes suivants :

a) $\begin{cases} n \equiv 1\ [20] \\ n \equiv 3\ [7] ; \end{cases}$ b) $\begin{cases} n \equiv 13\ [15] \\ n \equiv 6\ [10] ; \end{cases}$ c) $\begin{cases} n \equiv 11\ [15] \\ n \equiv 6\ [10] ; \end{cases}$ d) $\begin{cases} n \equiv 3\ [224] \\ n \equiv 17\ [119]. \end{cases}$

Solution

a) $\begin{cases} n \equiv 1\ [20] \\ n \equiv 3\ [7] ; \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 20a + 1 \\ \exists b \in \mathbb{Z},\ n = 7b + 3 \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 20a + 1 \\ \exists b \in \mathbb{Z},\ 20a + 1 = 7b + 3 \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 20a + 1 \\ \exists b \in \mathbb{Z},\ 20a - 7b = 2 \end{cases}$

$$\Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 20a + 1 \\ \exists b \in \mathbb{Z},\ 20a - 7b = 2(3 * 7 - 20) \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 20a + 1 \\ \exists b \in \mathbb{Z},\ 20(a + 2) = 7(b + 6) \end{cases} .$$

L'ensemble des solutions est par conséquent

$$\{140k - 39|\ k \in \mathbb{Z}\}.$$

b) $\begin{cases} n \equiv 13\ [15] \\ n \equiv 6\ [10] ; \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 15a + 13 \\ \exists b \in \mathbb{Z},\ 15a + 13 = 10b + 6 \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 15a + 13 \\ \exists b \in \mathbb{Z},\ 5(3a - 2b) = 6 - 13 \end{cases}$ or 5 ne divise pas 7 donc il n'y a pas de solution.

c) $\begin{cases} n \equiv 11\ [15] \\ n \equiv 6\ [10]\,; \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 15a + 13 \\ \exists b \in \mathbb{Z},\ 15a + 11 = 10b + 6 \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 15a + 13 \\ \exists b \in \mathbb{Z},\ 5(3a - 2b) = 6 - 11 \end{cases}$

$$\Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 15a + 13 \\ \exists b \in \mathbb{Z},\ (3a - 2b) = -1 \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 15a + 13 \\ \exists b \in \mathbb{Z},\ 3(a + 1) = 2(b + 1) \end{cases}.$$

L'ensemble des solutions est par conséquent

$$\{15(2k - 1) + 11|\ k \in \mathbb{Z}\} = \{30k - 4|\ k \in \mathbb{Z}\}.$$

d) $\begin{cases} n \equiv 3\ [224] \\ n \equiv 17\ [119]. \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 224a + 3 \\ \exists b \in \mathbb{Z},\ 224a - 119b = 14 \end{cases} \Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 224a + 3 \\ \exists b \in \mathbb{Z},\ 32a - 17b = 2 = 2 * 17 - 32 \end{cases}$

$$\Leftrightarrow \begin{cases} \exists a \in \mathbb{Z},\ n = 224a + 3 \\ \exists k \in \mathbb{Z},\ a + 1 = 17k \end{cases} \Leftrightarrow n \in \{224(17k - 1) + 3|\ k \in \mathbb{Z}\}.$$

<u>Exercice 11.</u>

1. Soit $(a, b) \in \mathbb{Z}^2$. Montrer que $\text{pgcd}(a, b) = 1$ si et seulement si $\text{pgcd}(a + b, ab) = 1$.
2. A-t-on, pour tout $(a, b) \in \mathbb{Z}^2$, $\text{pgcd}(a, b) = \text{pgcd}(a + b, ab)$?

Solution

1. $\Rightarrow$: Supposons que $\text{pgcd}(a, b) = 1$. Soit alors p un diviseur premier de $a + b$ et ab. Puisque $p|ab$ on a $p|a$ ou $p|b$. Dans les deux cas, puisque $p|a + b$, on récupère $p|a$ et $p|b$, ce qui est impossible. Donc les seuls diviseurs communs de $a + b$ et ab sont 1 et -1.

   $\Leftarrow$: Supposons que $\text{pgcd}(a, b) = d \neq 1$. Alors $d|a + b$ et $d|ab$ donc $d|\ \text{pgcd}(a + b, ab) \neq 1$.
2. Considérons $a = 2 = b$. On a $\text{pgcd}(a, b) = 2$ et $\text{pgcd}(a + b, ab) = 4$.

<u>Exercice 12.</u> Déterminer les valeurs de l'entier n pour lesquelles la fraction $\dfrac{n+2}{n+9}$ est irréductible ?

Solution

$$\begin{aligned} \frac{n+2}{n+9} \text{ est irréductible } &\Leftrightarrow \text{pgcd}(n + 2, n + 9) = 1 \\ &\Leftrightarrow \text{pgcd}(n + 9 - (n + 2), (n + 9)(n + 2)) = 1 \text{ en utilisant l'exercice précédent} \\ &\Leftrightarrow (7 \nmid (n + 2) \text{ et } 7 \nmid (n + 9)) \\ &\Leftrightarrow 7 \nmid (n + 2). \end{aligned}$$

Donc la fraction est irréductible si et seulement si n n'est pas congru à 5 modulo 7.

<u>Exercice 13.</u>

1. Soit $n > 1$ un nombre entier. Démontrer que, si $2^n + 1$ est premier, alors n est une puissance de 2.
2. Étant donné $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$; cet entier est appelé n-ième nombre de Fermat.
   (a) Calculer $F_0,\ F_1,\ F_2,\ F_3$ et F_4.
   (b) Démontrer que, pour tout $n \in \mathbb{N}$,

$$F_{n+1} = F_0 F_1 \cdots F_n + 2.$$

(c) En déduire que F_n et F_m sont premiers entre eux si m et n sont distincts.

3. Déduire de ce qui précède une démonstration de l'infinitude de l'ensemble des nombres premiers.

Solution

1. Soit p un diviseur impair de n. On pose $n = pk$; on a alors

$$2^n + 1 = (2^k)^p - (-1)^p = (2^k - 1)\sum_{i=0}^{p-1} 2^{ki} * (-1)^{p-1-i}.$$

On a donc $2^n + 1$ premier $\Rightarrow 2^k - 1 = 1$, c'est-à-dire $k = 1$. Puisque le seul diviseur impair de n est 1, n est une puissance de 2.

2. (a) $F_0 = 3$; $F_1 = 5$; $F_2 = 17$; $F_3 = 257$; $F_4 = 65537$.

   (b) On procède ici par récurrence : $F_1 = F_0+2$. De plus, si $n \in \mathbb{N}$ est tel que $F_{n+1} = F_0F_1 \cdots F_n+2$, on a

$$\begin{aligned} F_{n+2} - 1 &= 2^{2^{n+2}} \\ &= (2^{2^{n+1}})^2 \\ &= (F_{n+1} - 1)^2 \\ &= F_{n+1}(F_{n+1} - 1) - F_{n+1} + 1 \\ &= F_{n+1}(F_0F_1 \cdots F_n + 1) - F_{n+1} + 1 \text{ via l'hypothèse de récurrence} \\ &= F_0F_1 \cdots F_nF_{n+1} + 1 \end{aligned}$$

   On a donc bien, pour tout entier n, $F_{n+1} = F_0F_1 \cdots F_n + 2$.

   (c) Soit n et m deux entiers distincts. On suppose, sans perte de généralité, que $n < m$. On peut alors écrire $F_m = F_{m-1} \cdots F_0 + 2 = kF_n + 2$ pour un entier k. Soit alors d un diviseur commun de F_n et F_m. On a alors

$$d|F_n \text{ et } d|2.$$

   En se servant de la forme de F_n, ceci implique $d = 1$ ou $d = -1$; donc $\text{pgcd}(F_n, F_m) = 1$.

3. Posons, pour tout entier n, p_n un diviseur premier de F_n (par définition il en existe toujours au moins un). Alors, la question précédente nous certifie que les nombres p_n sont deux-à-deux distincts, donc l'ensemble $\{p_n|n \in \mathbb{N}\}$ fourni une infinité de nombres premiers.

Exercice 14.

1. Donner la décomposition en facteurs premiers de 12.
2. Énumérer les diviseurs de 12.

Solution

1. $12 = 2^2 * 3$.
2. Les diviseurs de 12 sont donc : 1, 2, 3, 4, 6, 12, ainsi que leurs opposés : -1, -2, $\cdots$.

Exercice 15.

1. Soit $N \in \mathbb{N}^*$. Exprimer à l'aide de la décomposition en facteurs premiers de N le nombre $\sigma_0(N)$ de diviseurs positifs de N et leur somme $\sigma_1(N)$.
2. Déterminer l'ensemble des entiers positifs possédant 6 diviseurs positifs dont la somme est 28.

Solution

1. Écrivons $N = \prod_{k=1}^{r} p_k^{a_k}$. Les diviseurs de N sont alors les $\prod_{k=1}^{r} p_k^{b_k}$ où pour tout k on a $0 \leq b_k \leq a_k$. Il s'agit alors de dénombrer ceux-ci : il y en a $\prod_{k=1}^{r} (a_k+1)$. Pour s'en convaincre, il suffit de considérer la bijection qui, à un diviseur $\prod_{k=1}^{r} p_k^{b_k}$ de N, associe le r-uplet $(b_1, b_2, \cdots, b_r)$. L'ensemble d'arrivée de cette bijection est alors $\{0,1,\cdots,a_1\} \times \cdots \times \{0,1,\cdots,a_r\}$.
Regardons maintenant $\sigma_1(N)$. On a :

$$\begin{aligned}
\sigma_1(N) &= \sum_{(b_1,\cdots,b_r)\in\{0,1,\cdots,a_1\}\times\cdots\times\{0,1,\cdots,a_r\}} \prod_{k=1}^{r} p_k^{b_k} \\
&= \sum_{b_1=0}^{a_1} \sum_{(b_2,\cdots,b_r)\in\{0,1,\cdots,a_2\}\times\cdots\times\{0,1,\cdots,a_r\}} p_1^{b_1} \prod_{k=2}^{r} p_k^{b_k} \\
&= \sum_{b_1=0}^{a_1} p_1^{b_1} (\sum_{(b_2,\cdots,b_r)\in\{0,1,\cdots,a_2\}\times\cdots\times\{0,1,\cdots,a_r\}} \prod_{k=2}^{r} p_k^{b_k}) \\
&= \frac{1-p_1^{a_1+1}}{1-p_1} \sum_{(b_2,\cdots,b_r)\in\{0,1,\cdots,a_2\}\times\cdots\times\{0,1,\cdots,a_r\}} \prod_{k=2}^{r} p_k^{b_k} \\
&= \prod_{k=1}^{r} \frac{1-p_k^{a_k+1}}{1-p_k}
\end{aligned}$$

2. On a $6 = 2*3$ donc les entiers N recherchés sont de la forme $N = p_1 p_2^2$ avec p_1 et p_2 deux nombres premiers. On a alors $(1+p_1)(1+p_2+p_2^2) = 28 = 7*4$. Une recherche exhaustive donne alors $p_1 = 3$ et $p_2 = 2$. Donc $N = 12$ est la seule solution à notre problème.

Exercice 16. Montrer que pour tout entier n, $n^5 - n$ est divisible par 15.
Solution

$$\begin{aligned}
n^5 - n = n(n^4-1) &= n(n-1)(n^3+n^2+n+1) \\
&= n(n-1)(n^3-n+(n+1)^2) \\
&= n(n-1)(n(n-1)(n+1)+(n+1)^2) \\
&= n(n-1)(n+1)(n^2+1)
\end{aligned}$$

On a déjà $3|n(n-1)(n+1)$ puisque sur trois entiers consécutifs, l'un est nécessairement multiple de 3. D'autre part, si $5 \nmid n(n-1)(n+1)$, on a $n \equiv 2\,[5]$ ou $n \equiv 3\,[5]$. Les deux cas donnent $n^2+1 \equiv 0\,[5]$. D'où le résultat énoncé.

Exercice 17. Montrer que $p^2 \equiv 1 \mod 24$ pour tout nombre premier p supérieur ou égal à 5.
Solution
On a $p^2 - 1 = (p-1)(p+1)$. Pour p premier supérieur à 5, p est impair. Donc $p-1$ et $p+1$ sont deux entiers pairs consécutifs, ainsi l'un d'entre eux est un multiple de 4. Donc 8 divise p^2-1. D'autre part, puisque les entiers $p-1$, p et $p+1$ sont consécutifs, l'un des trois des multiple de 3 ; or ce n'est pas p puisqu'il est premier et que ce n'est pas 3. On a aussi $3|(p^2-1)$. D'où, puisque 3 et 8 sont premiers entre eux, on a $24|p^2-1$.

Exercice 18. Montrer que pour tous $n \in \mathbb{N}$, et $a, b \in \mathbb{Z}$, si $a \equiv b \mod n$ alors $a^n \equiv b^n \mod n^2$.

Solution

Pour a et $b \in \mathbb{Z}$, on a $a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}$. Donc si $a \equiv b \mod n$, on a $n|(a-b)$ et $a^k b^{n-1-k} \equiv a^{n-1} \mod n$. D'où $\sum_{k=0}^{n-1} a^k b^{n-1-k} \equiv \sum_{k=0}^{n-1} a^{n-1} \mod n$ donc $n | \sum_{k=0}^{n-1} a^k b^{n-1-k}$. D'où $n^2 | a^n - b^n$.

Exercice 19. Soit $(u_n)_{n\in\mathbb{N}}$ une suite non-négative sous-additive, i.e. pour laquelle $u_{m+n} \leq u_m + u_n$ pour tous $m, n \in \mathbb{N}$. On pose $A = \{\frac{u_n}{n} : n \in \mathbb{N}^*\}$.

1. Soient $n, N \in \mathbb{N}^*$. La division euclidienne de n par N s'écrit $n = Nq + r$ pour certains $q, r \in \mathbb{N}$ avec $r < N$. Montrer que
$$\frac{u_n}{n} \leq \frac{u_N}{N} + \frac{u_r}{n}.$$
2. En déduire que pour tout $\epsilon > 0$ et $N \in \mathbb{N}^*$ on a $\frac{u_n}{n} \leq \frac{u_N}{N} + \epsilon$ à partir d'un certain rang.
3. En déduire que $\lim_{n\to\infty} \frac{u_n}{n} = \inf A$.

Solution

1. $$\begin{aligned}\frac{u_n}{n} &\leq \frac{u_{qN}}{n} + \frac{u_r}{n} \text{ par sous-additivité}\\ &\leq \frac{qu_N}{n} + \frac{u_r}{n} \text{ par récurrence et sous-additivité}\\ &= \frac{qu_N}{qN+r} + \frac{u_r}{n}\\ &\leq \frac{qu_N}{qN} + \frac{u_r}{n} \text{ par non-négativité}\\ &= \frac{u_N}{N} + \frac{u_r}{n}.\end{aligned}$$
2. Pour un entier r quelconque, on déjà vu qu'une induction donne $u_r \leq ru_1$. Aussi, en reprenant le résultat précédent, pour avoir $\frac{u_n}{n} \leq \frac{u_N}{N} + \epsilon$, il suffit d'avoir $\frac{u_r}{n} \leq \epsilon$ c'est-à-dire $u_1\frac{r}{n} \leq \epsilon$ donc il suffit de prendre $n > \frac{u_1 N}{\epsilon}$.
3. Notons $l = infA$, qui existe et est supérieur ou égal à 0. Soit alors $\epsilon > 0$ et soit N tel que $\frac{u_N}{N} < l + \frac{\epsilon}{2}$. Soit M le rang donné par la question précédente tel que
$$\forall n > M, \frac{u_n}{n} \leq \frac{u_N}{N} + \frac{\epsilon}{2} \leq l + \epsilon.$$
Donc, puisque l est l'infimum de A, on a $n > M \implies |\frac{u_n}{n} - l| \leq \epsilon$.

Exercice 20. Montrer que $\frac{\ln a}{\ln b}$ est irrationnel pour tous a, b premiers entre eux.

Solution

Supposons pgcd$(a, b) = 1$ et qu'il existe c et d deux entiers premiers entre eux tels que $\frac{\ln a}{\ln b} = \frac{c}{d}$. O suppose de plus que $a > 1$ et $b > 1$, sinon le résultat est soit clairement faux (cas $a = 1$ et $b > 1$), soit n'a pas de sens.
Alors $d \ln a = c \ln b$ donc $a^d = b^c$. Mais, pour p premier divisant a, on a $p|b^c$ et donc $p|b$, en contradiction avec pgcd$(a, b) = 1$.

Exercice 21.

1. Soient $a, b \in \mathbb{N}$ et $k \geq 2$ entier. Montrer que si a et b sont premiers entre eux et si ab est la puissance l-ème d'un entier, alors a et b sont eux-mêmes des puissances l-èmes d'entiers.
2. Le résultat précédent est-il vrai pour des entiers $a, b \in \mathbb{Z}$?

Solution

1. On écrit $a = \prod_{k=1}^{n} p_k^{a_k}$ et $b = \prod_{k=1}^{n} p_k^{b_k}$, où si $a_k \neq 0$ on a $b_k = 0$ et réciproquement. Alors on a
$$ab = \prod_{k=1}^{n} p_k^{\max(a_k,b_k)} = c^l = \prod_{k=1}^{n} p_k^{l*c_k}.$$
On en déduit que les a_k et les b_k sont des multiples de l, donc $a = (\prod_{k=1}^{n} p_k^{\frac{a_k}{l}})^l$ et $b = (\prod_{k=1}^{n} p_k^{\frac{b_k}{l}})^l$ sont bien des puissances l-ièmes.
2. On voit, en prenant $a = b = -1$ qu'on peut avoir $ab = 1 = 1^2$ mais pourtant ni a ni b ne sont des carrés.

Exercice 22. Soient $x, y, z \in \mathbb{N}^*$. On suppose que $x^2 + y^2 = z^2$ et $\mathrm{pgcd}(x, y) = 1$.

1. Montrer que $\mathrm{pgcd}(y, z) = 1$.
2. Montrer que x ou y est pair. Quitte à les permuter, on suppose désormais y pair.
3. Montrer que $y+z$ et $z-y$ sont premiers entre eux, puis que $y+z = a^2$ et $z-y = b^2$ pour certains $a, b \in \mathbb{N}^*$ impairs et premiers entre eux.
4. En déduire la forme du triplet (x, y, z).

Solution

1. Soit $p = \mathrm{pgcd}(y, z)$. Alors $p|y^2$ et $p|z^2$ donc $p|x^2$ puisque $x^2 = z^2 - y^2$. Mais alors $p|\,\mathrm{pgcd}(x, y)$.
2. Si $x = 2k+1$ et $y = 2k'+1$, alors $z^2 = 4(k^2 + k'^2 + k + k') + 2 \equiv 2 \pmod 4$. Donc z est pair, mais z^2 devrait alors être un multiple de 4. De plus, on peut remarquer que si y pair, x doit alors nécessairement être impair pour avoir $\mathrm{pgcd}(x, y) = 1$.
3. Soit p premier tel que $p|y+z$ et $p|z-y$. Alors $p^2|(z+y)(z-y)$, c'est-à-dire x^2 : puisque x est impair, $p \neq 2$. On a aussi $p|z+y+z-y$ c'est-à-dire $p|2z$, et $p|z+y-z+y$ c'est-à-dire $p|2y$. Finalement, on a $p|\,\mathrm{pgcd}(y, z)$ ce qui est impossible.
On réutilise alors l'exercice précédent : $(z+y)(z-y) = x^2$ donc $z+y$ et $z-y$ sont des carrés. Puisque z est impair et y est pair, on a bien a et b impairs, et ils sont premiers entre eux puisque leurs carrés sont premiers entre eux.
4. Le triplet est de la forme $(ab, \frac{a^2-b^2}{2}, \frac{a^2+b^2}{2})$.

Exercice 23. On cherche à résoudre l'équation diophantienne $x^y = y^x$ d'inconnues $x, y \in \mathbb{N}^*$.

1. On suppose que $x \leq y$. Montrer que $x \mid y$, en factorisant x et y en produits de puissances de nombres premiers.
2. Écrire $y = xz$, et montrer que $xz = x^z$.
3. Étudier les variations de la fonction réelle $f(z) = z^{\frac{1}{z-1}}$ pour $z \geq 2$.
4. Montrer que si $z \geq 2$ est entier avec $f(z)$ entier, alors $z = 2$.
5. En déduire que les seules solutions entières de $x^y = y^x$ sont $x = y \in \mathbb{N}^*$ et $x = 2$, $y = 4$, ou $x = 4$, $y = 2$.

Solution

1. On écrit $x = \prod_{k=1}^{n} p_k^{a_k}$ et $y = \prod_{k=1}^{n} p_k^{b_k}$, où a_k et b_k peuvent être nuls. Alors

$$x^y = \prod_{k=1}^{n} p_k^{ya_k} = y^x = \prod_{k=1}^{n} p_k^{xb_k}.$$

D'où, pour tout k, $ya_k = xb_k$ et donc $b_k = \frac{y}{x}a_k \geq a_k$, ce qui signifie exactement que $x|y$.

2. On a $(xz)^x = x^{xz} = (x^z)^x$. Par injectivité des fonctions logarithme et exponentielle, on récupère $xz = x^z$.
3. Pour $z \geq 2$, f est dérivable de dérivée $z \to \frac{z-1-z\ln(z)}{z(z-1)^2} z^{\frac{1}{z-1}}$ strictement négative sur $[2,+\infty[$. De plus, $\lim_{z \to +\infty} f(z) = e^0 = 1$.
4. Soit $n = f(z)$. On a $2 = f(2) \geq n > 1$ d'après les variations de f. Donc $n = 2$ et $z = 2$.
5. Puisqu'on est sur $\mathbb{N}^*$ et que $z \geq 2$ si $x < y$ on a

$$xz = x^z \Leftrightarrow z = x^{z-1} \Leftrightarrow f(z) = x.$$

Ceci est possible uniquement pour $z = 2$, qui donne $x = 2$ et $y = xz = 4$. Bien sûr, la solution symétrique obtenue si $y < x$ est $x = 4$ et $y = 2$.

Exercice 24. Déterminer le PGCD des paires suivantes de nombres naturels en ne vous servant que de la division euclidienne.

$$(252, 75) \quad (300, 504) \quad (12375, 1815)$$

Écrire une identité de Bezout pour chaque paire.

Solution Nous donnons la correction entière pour la première paire et nous nous contenterons de fournir les PGCD et des identités de Bezout qui découlent de la méthode qui aura été illustrée dans la correction de la première paire.

$$\begin{aligned}
252 &= 3 \times 75 + 27 && (1)\\
75 &= 2 \times 27 + 21 && (2)\\
27 &= 1 \times 21 + 6 && (3)\\
21 &= 3 \times 6 + 3 && (4)\\
6 &= 2 \times 3. && (5)
\end{aligned}$$

La dernière égalité où le reste est 0 montre que le PGCD est 3.
Pour l'identité de Bezout on remonte les égalités dans le sens inverse à partir de l'égalité (4) où apparaît le PGCD comme le reste :

$$\begin{aligned}
3 &= 21 - 3 \times 6\\
&= 21 - 3 \times (27 - 1 \times 21)\\
&= -3 \times 27 + 4 \times 21\\
&= -3 \times 27 + 4 \times (75 - 2 \times 27)\\
&= 4 \times 75 - 11 \times 27\\
&= 4 \times 75 - 11 \times (252 - 3 \times 75)\\
&= -11 \times 252 + 37 \times 75.
\end{aligned}$$

Pour la deuxième paire soit on peut constater que 4 est un diviseur commun et faire le travail avec $(126, 75)$ quitte à multiplier le PGCD par 4 à la fin, soit on fait directement comme dans le cas de la

paire précédente. On trouve alors que le PGCD de 504 et 300 est 12.L'identité Bezout qui découle de la méthode utilisée pour la première paire est $12 = 3 \times 504 - 5 \times 300$.
Les mêmes remarques que celles du paragraphe précédent s'appliquent à la dernière paire. On trouve alors que le PGCD de $(12375, 1815)$ est 165. L'identité Bezout qui en découle si on suit la méthode illustrée ci-dessus, est $165 = 5 \times 12375 - 34 \times 1815$.