

ARITHMÉTIQUE

SOLUTION 1.

Dans ce qui suit toutes les congruences sont modulo 7.

Soient x et y divisibles par 7. Alors $x \equiv y \equiv 0$ et $x^2 + y^2 \equiv 0^2 + 0^2 \equiv 0$.

Pour la réciproque, supposons que $x^2 + y^2 \equiv 0^2 + 0^2 \equiv 0$. Or pour un carré il n'y a que quatre valeurs possibles 0, 1, 2 et 4. En effet :

- Si $x \equiv 0$ alors $x^2 \equiv 0$,
- Si $x \equiv \pm 1$ alors $x^2 \equiv 1$,
- Si $x \equiv \pm 2$ alors $x^2 \equiv 4$,
- Si $x \equiv \pm 3$ alors $x^2 \equiv 9 \equiv 2$.

Donc la somme de deux carrés ne peut être 0 modulo 7 que si $x \equiv y \equiv 0$.

SOLUTION 2.

1. On a modulo 17 :

$$7^2 \equiv 49 \equiv -2 \Rightarrow 7^4 \equiv (-2)^2 \equiv 4 \Rightarrow 7^8 \equiv 4^2 \equiv -1.$$

Ainsi

$$\begin{aligned} 7^{8n+1} + 10(-1)^n &\equiv 7(7^8)^n + 10(-1)^n \\ &\equiv 7(-1)^n + 10(-1)^n \\ &\equiv 17(-1)^n \equiv 0. \end{aligned}$$

2. On calcule modulo 11 :

$$\begin{aligned} 9^{5n+2} - 4 &\equiv (-2)^{5n+2} - 4 \equiv 4((-2)^5)^n - 4 \\ &\equiv 4[(-32)^n - 1] \equiv 4[1^n - 1] \equiv 0. \end{aligned}$$

3. Il est clair que pour tout $n \in \mathbb{N}$ le nombre $10^{3n+2} - 4^{n+1}$ est divisible par 2. Il suffit alors de montrer qu'il est également divisible par

3. On trouve modulo 3 :

$$10^{3n+2} - 4^{n+1} \equiv 1^{3n+2} - 1^{n+1} \equiv 1 - 1 \equiv 0.$$

SOLUTION 3.

Oui ! On calcule

$$a_1 = 1$$

$$a_5 = 153$$

$$a_2 = 3$$

$$a_6 = 873$$

$$a_3 = 9$$

$$a_7 = 5913$$

$$a_4 = 33$$

$$a_8 = 46233$$

On a $a_5 = 9 \times 17$, et puisque pour tout $k \geq 6$ la factorielle $k!$ est multiple de 9 on déduit

$$\forall n \geq 5 \quad a_n = a_5 + \sum_{k=6}^n k! \equiv 0 \pmod{9}.$$

On calcule

$$\frac{a_8}{9} = 5137.$$

Puisque 5137 n'est pas un multiple de trois on en déduit que a_8 n'est pas un multiple de 27. D'autre part pour tout $k \geq 9$ la factorielle $k!$ est multiple de 27.

$$\forall n \geq 8 \quad a_n = a_8 + \sum_{k=9}^n k! \equiv a_8 \not\equiv 0 \pmod{27}.$$

On peut donc affirmer que a_n est divisible par 9 et non-divisible par 27 à partir du rang $n = 8$.

SOLUTION 4.

On utilise la formule du binôme :

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

Dès que $k \geq 2$, n^2 divise n^k . De plus, $\binom{n}{1} = n$ donc n^2 divise tous les termes de la somme précédente et donc divise $(n+1)^n - 1$.

SOLUTION 5.

Raisonnons par récurrence sur n .

La propriété est évidente au rang $n = 0$. Supposons-la vraie à un certain rang $n \in \mathbb{N}$. Remarquons que

$$5^{2^{n+1}} - 1 = (5^{2^n})^2 - 1 = (5^{2^n} - 1)(5^{2^n} + 1)$$

D'après l'hypothèse de récurrence 2^{n+2} est la plus grande puissance de 2 divisant $5^{2^n} - 1$.

Montrons que 2 est la plus grande puissance de 2 divisant $5^{2^n} + 1$. On sait que $5 \equiv 1[4]$. Donc $5^{2^n} + 1 \equiv 2[4]$. Ceci prouve que 2 divise $5^{2^n} + 1$ mais que 4 ne le divise pas.

En conclusion, 2^{n+3} est la plus grande puissance de 2 divisant $5^{2^{n+1}} - 1$.

SOLUTION 6.

Soit a un entier. Soit a_0, a_1, \dots, a_n les chiffres composant a de sorte que $a = \sum_{k=0}^n a_k 10^k$.

1. On remarque que $10 \equiv 1[3]$. Donc pour tout $k \in \llbracket 0, n \rrbracket$, $10^k \equiv 1[3]$. Par conséquent, $a \equiv \sum_{k=0}^n a_k [3]$. On en déduit donc que a est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.
2. On remarque que $10 \equiv 1[9]$. Donc pour tout $k \in \llbracket 0, n \rrbracket$, $10^k \equiv 1[9]$. Par conséquent, $a \equiv \sum_{k=0}^n a_k [9]$. On en déduit donc que a est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.
3. On remarque que $10 \equiv -1[11]$. Donc pour tout $k \in \llbracket 0, n \rrbracket$, $10^k \equiv (-1)^k [11]$. Par conséquent, $a \equiv \sum_{k=0}^n (-1)^k a_k [11] \equiv \sum_{0 \leq 2k \leq n} a_k - \sum_{0 \leq 2k+1 \leq n} a_{2k+1} [11]$. On en déduit donc que a est divisible par 11 si et seulement si la somme de ses chiffres de rang pair moins la somme de ses chiffres de rang impair est divisible par 11.

SOLUTION 7.

1. $2^5 \equiv 2[5]$ et $2^3 \equiv 3[5]$ donc $2^{3n} \equiv 3^n[5]$. Par conséquent, $2^{3n+5} \equiv 2 \cdot 3^n[5]$. Enfin,

$$2^{3n+5} + 3^{n+1} \equiv 2 \cdot 3^n + 3 \cdot 3^n \equiv 0[5]$$

2. D'après le théorème de Fermat, $n^5 \equiv n[5]$. Donc 5 divise $n^5 - n$. En utilisant à nouveau Fermat, on a $n^3 \equiv n[3]$. D'où $n^5 \equiv n^3 \equiv n[3]$. Ainsi 3 divise $n^5 - n$. Enfin, n^5 et n ont même parité donc $n^5 - n$ est pair i.e. 2 divise $n^5 - n$. Ainsi $n^5 - n$ est divisible par 2, 3 et 5 qui sont premiers entre eux deux à deux donc $n^5 - n$ est divisible par $2 \times 3 \times 5 = 30$.

SOLUTION 8.

L'ensemble de l'énoncé est formé des entiers de la forme $u_n = \sum_{k=0}^n 10^k$ pour $n \in \mathbb{N}$. On a facilement $u_n = \frac{1}{9}(10^{n+1} - 1)$. Remarquons que si $p = 3$, alors p divise 111 par exemple.
 Soit p un entier premier différent de 2, 3 et 5. Alors $10 = 2 \times 5$ est premier avec p . D'après le petit théorème de Fermat, $10^{p-1} \equiv 1 \pmod{p}$ donc p divise $10^{p-1} - 1$. Comme $p \neq 3$, p est premier avec 9. On sait que 9 divise $10^{p-1} - 1$ puisque $\frac{1}{9}(10^{p-1} - 1) = u_{p-2} \in \mathbb{N}$. Donc $9p$ divise $10^{p-1} - 1$ i.e. p divise u_{p-2} .

SOLUTION 9.

1. Soit $n \in \mathbb{N}$. Soit r le chiffre des unités de n . Il existe alors $m \in \mathbb{N}$ tel que $n = 10m + r$. On conclut en remarquant que $n \equiv r[5]$ puisque $10 \equiv 0[5]$ et que les seuls chiffres (i.e. entiers compris entre 0 et 9) divisibles par 5 sont 0 et 5.
2. Soit $n \in \mathbb{N}$. Soit r l'entier formé par les deux derniers chiffres de n . Il existe alors $m \in \mathbb{N}$ tel que $n = 100m + r$. On conclut en remarquant que $n \equiv r[4]$ puisque $100 \equiv 0[4]$.

SOLUTION 10.

On fixe un entier a impair et on fait l'hypothèse de récurrence suivante :

$$\text{HR}(n) : a^{2^{n-1}} \equiv 1[2^n]$$

Initialisation : On sait que a est impair donc $a - 1$ et $a + 1$ sont pairs et $a^2 - 1 = (a - 1)(a + 1)$ est donc divisible par 4 i.e. $a^2 \equiv 1[4]$ de sorte que $\text{HR}(2)$ est vraie.

Hérédité : Supposons $\text{HR}(n)$ vraie pour un certain $n \in \mathbb{N}$. Alors $a^{2^{n-1}} - 1$ est divisible par 2^n . De plus $a^{2^{n-1}} + 1$ est pair car a est impair. Ainsi $a^{2^n} - 1 = (a^{2^{n-1}} - 1)(a^{2^{n-1}} + 1)$ est divisible par $2^n \times 2 = 2^{n+1}$ i.e. $a^{2^n} \equiv 1[2^{n+1}]$ de sorte que $\text{HR}(n + 1)$ est vraie.

Conclusion : Par récurrence, $\text{HR}(n)$ est vraie pour tout entier $n \geq 2$.

SOLUTION 11.

Puisque 10 et 13 sont premiers entre eux, ils vérifient une relation de Bézout. En effet, $4 \times 10 - 3 \times 13 = 1$. Par conséquent, $12 \times 10 - 9 \times 13 = 3$ ou encore $122 = 2 + 12 \times 9 = 5 + 9 \times 13$. Ainsi 122 est solution particulière.

$$\begin{aligned} \begin{cases} x \equiv 2[10] \\ x \equiv 5[13] \end{cases} &\iff \begin{cases} x \equiv 122[10] \\ x \equiv 122[13] \end{cases} \\ &\iff \begin{cases} 10 \mid x - 122 \\ 13 \mid x - 122 \end{cases} \\ &\iff 130 \mid x - 122 \quad \text{car } 10 \wedge 13 = 1 \\ &\iff x \equiv 122[130] \end{aligned}$$

L'ensemble des solutions est donc $122 + 130\mathbb{Z}$.

SOLUTION 12.

1. Si le système admettait des solutions, il existerait $k, l \in \mathbb{Z}$ tel que $3 + 10k = 4 + 8l$ i.e. $10k - 8l = 1$. Ceci est impossible puisque 2 divise $10k - 8l$ et pas 1.

2. Le système admet des solutions *si et seulement si* il existe $(k, l) \in \mathbb{Z}^2$ tel que $a + 10k = b + 8l$ i.e. $10k - 8l = b - a$. Comme $10 \wedge 8 = 2$, ceci équivaut à $2 \mid b - a$.
3. On a $10 - 8 = 2$ et donc $-6 = 2 - 8 = 4 - 10$. Ceci signifie que -6 est une solution particulière.

$$\begin{aligned} \begin{cases} x \equiv 4[10] \\ x \equiv 2[8] \end{cases} &\iff \begin{cases} x \equiv -6[10] \\ x \equiv -6[8] \end{cases} \\ &\iff \begin{cases} 10 \mid x + 6 \\ 8 \mid x + 6 \end{cases} \\ &\iff 40 \mid x + 6 \quad \text{car } 10 \vee 8 = 40 \\ &\iff x \equiv -6[40] \end{aligned}$$

L'ensemble des solutions est donc $-6 + 40\mathbb{Z}$.

SOLUTION 13.

1. Le nombre $2^{2^{10}}$ est tellement grand qu'on ne peut pas effectuer cette division sans astuce (ou ordinateur). On essaie donc d'abord de voir ce qui se passe avec des exposants petits. On a les équivalences suivantes modulo 7 : $2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 2$ et $2^3 \equiv 1$. Donc il y a un cycle de longueur 3 pour les exposants. Ainsi je la division euclidienne de 2^{10} par 3,

$$2^{10} = 3q + r,$$

ce qui permet d'écrire

$$2^{2^{10}} \equiv 2^{3q+r} \equiv (2^3)^q \times 2^r \equiv 2^r \pmod{7}.$$

Il reste alors à déterminer ce reste r . Trois méthodes pour cela :

- Par calcul mental. $2^{10} = 1024 = 341 \times 3 + 1$.
- Les parésseux reconnaissent que 1023 est divisible par 3, donc le reste est 1.
- On écrit $2^{10} \equiv 2^{2 \times 5} \equiv (2^2)^5 \equiv 4^5 \equiv 1^5 \equiv 1 \pmod{3}$.

On obtient alors

$$2^{2^{10}} \equiv 2 \pmod{7}$$

ce qui prouve que reste de la division euclidienne de $2^{2^{10}}$ par 7 est 2.

2. Imitant la méthode ci-dessus nous cherchons une puissance 3^n équivalente à $\pm 1 \pmod{25}$.

$$\begin{aligned} 3^2 &\equiv 9, \quad 3^3 \equiv 2, \quad 3^4 \equiv 6, \quad 3^5 \equiv -7, \quad 3^6 \equiv 4, \\ 3^7 &\equiv 12, \quad 3^8 \equiv 11, \quad 3^9 \equiv 8, \quad 3^{10} \equiv -1 \pmod{25}. \end{aligned}$$

Comme $2189 = 10 \times 218 + 9$ on trouve

$$3^{2189} \equiv (3^{10})^{218} \times 3^9 \equiv (-1)^{218} \times 8 \equiv 8 \pmod{25}.$$

SOLUTION 14.

1. On a $a^n = a^r(a^{mq} - 1) + a^r$ et

$$a^{mq} - 1 = (a^m)^q - 1 = (a^m - 1) \sum_{k=0}^{q-1} (a^m)^k$$

donc $a^{mq} - 1$ est divisible par $a^m - 1$ et $a^n \equiv a^r[a^m - 1]$.

On peut également remarquer que $a^m \equiv 1[a^m - 1]$ donc $a^{qm} \equiv 1[a^m - 1]$ donc $a^{qm+r} \equiv a^r[a^m - 1]$ i.e. $a^n \equiv a^r[a^m - 1]$.

2. Remarquons que

$$a^n - 1 \equiv a^r - 1 [a^m - 1] \text{ et } 0 \leq a^r - 1 < a^m - 1$$

car $r < q$ et $a > 1$. Ainsi $a^r - 1$ est le reste de la division euclidienne de $a^n - 1$ par $a^m - 1$. Par conséquent,

$$d = (a^n - 1) \wedge (a^m - 1) = (a^m - 1) \wedge (a^r - 1).$$

On définit la suite d'entiers (r_k) par $r_0 = n$, $r_1 = m$ et si r_{k+1} est non nul, r_{k+2} est le reste de la division euclidienne de r_k par r_{k+1} i.e. on applique l'algorithme d'Euclide à n et m . On sait qu'il existe K tel que $r_K = n \wedge m$ et $r_{K+1} = 0$. D'après ce qui précède, on démontre par récurrence que $(a^{r_k} - 1)$ est la suite des entiers définis par l'algorithme d'Euclide appliqué à $a^n - 1$ et $a^m - 1$. Comme $a^{r_{K+1}} - 1 = 0$, c'est que $a^{r_K} - 1 = a^{n \wedge m} - 1$ est le pgcd de $a^n - 1$ et $a^m - 1$.

3. $a^m - 1$ divise $a^n - 1$ si et seulement si $(a^n - 1) \wedge (a^m - 1) = a^m - 1$, ou encore si et seulement si $a^{n \wedge m} - 1 = a^m - 1$. Comme $a > 1$, ceci équivaut à $n \wedge m = m$ i.e. m divise n .

SOLUTION 15.

On peut considérer toutes les possibilités de reste de la division euclidienne de a par 8 mais la démonstration suivante montre que l'on peut se limiter aux restes modulo 4.

- Si $a \equiv 0[4]$, il existe $k \in \mathbb{Z}$ tel que $a = 4k$. Alors $a^2 = 16k^2 = 8 \times 2k^2 + 0$ et donc le reste est 0.
- Si $a \equiv 1[4]$, il existe $k \in \mathbb{Z}$ tel que $a = 4k + 1$. Alors $a^2 = 16k^2 + 8k + 1 = 8 \times (2k^2 + k) + 1$ et donc le reste est 1.
- Si $a \equiv 2[4]$, il existe $k \in \mathbb{Z}$ tel que $a = 4k + 2$. Alors $a^2 = 16k^2 + 16k + 4 = 8 \times (2k^2 + 2k) + 4$ et donc le reste est 4.
- Si $a \equiv 3[4]$, il existe $k \in \mathbb{Z}$ tel que $a = 4k + 3$. Alors $a^2 = 16k^2 + 24k + 9 = 8 \times (2k^2 + 3k + 1) + 1$ et donc le reste est 1.

SOLUTION 16.

On écrit la division euclidienne de $a - 1$ par b : $a - 1 = bq + r$ avec $0 \leq r \leq b - 1$. Pour $n \in \mathbb{N}$, on a donc

$$ab^n - b^n = b^{n+1}q + rb^n$$

Par conséquent,

$$ab^n - 1 = b^{n+1}q + (r + 1)b^n - 1$$

Par ailleurs, $0 \leq r \leq b - 1$ donc $1 \leq r + 1 \leq b$ et donc $0 \leq (r + 1)b^n - 1 \leq b^{n+1} - 1$. Ceci prouve que le quotient de la division euclidienne de $ab^n - 1$ par b^{n+1} est q .

SOLUTION 17.

On écrit $n^2 + 1 = (n - 1)(n + 1) + 2$. Ainsi dès que $n \geq 2$, 2 est le reste de la division euclidienne de $n^2 + 1$ par $n + 1$. 2 étant notoirement non nul, $n + 1$ ne divise pas $n^2 + 1$.

1 est le seul entier n tel que $n + 1$ divise $n^2 + 1$.

SOLUTION 18.

On remarque que $2^3 \equiv 1[7]$. De plus, $2009 = 3 \times 669 + 2$. Donc $2^{2009} \equiv 2^2[7]$. Comme $0 \leq 4 < 7$, le reste de la division euclidienne de 2^{2009} par 7 est 4.

SOLUTION 19.

D'après le théorème de Bezout, il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $au - bv = 1$. On effectue la division euclidienne de u par b et de v par a de sorte que $u = bq + u_0$ avec $0 \leq u_0 < b$ et $v = ar + v_0$ avec $0 \leq v_0 < a$. On a alors :

$$au - bv = ab(q - r) + au_0 - bv_0 = 1$$

On a de plus $0 \leq u_0 \leq b - 1$ et $0 \leq v_0 \leq a - 1$ donc $-ab + b \leq au_0 - bv_0 \leq ab - a$. On en déduit que

$$-ab + a + 1 \leq ab(q - r) \leq ab - b + 1$$

Comme $a \geq 0$ et $b \geq 2$, $-ab < ab(q - r) < ab$ et donc $-1 < q - r < 1$. C'est donc que $q = r$ et $au_0 - bv_0 = 1$.

Reste à montrer l'unicité. Soit $(u_1, v_1) \in \mathbb{N}^2$ vérifiant :

$$u_1 a - v_1 b = 1$$

$$u_1 < b$$

$$v_1 < a$$

On a alors $(u_1 - u_0)a = (v_1 - v_0)b$. Le théorème de Gauss nous dit que $u_1 - u_0$ est un multiple de b . Mais $-b < u_1 - u_0 < b$. C'est donc que $u_0 = u_1$. On démontre de même que $v_0 = v_1$.

SOLUTION 20.

- On applique la méthode de résolution des équations diophantiennes du type $ax + by = c$.

Simplification par le pgcd Le pgcd de 221 et 247 est 13 (on le trouve en utilisant l'algorithme d'Euclide). L'équation est alors équivalente à $17x + 19y = 4$ avec 17 et 19 premiers entre eux.

Recherche d'une solution particulière Ici, on a clairement $-17 + 19 = 2$ donc $17 \times (-2) + 19 \times 2 = 4$. Le couple $(-2, 2)$ est donc une solution particulière.

Recherche de la solution générale

$$\begin{aligned} 17x + 19y = 4 &\iff 17x + 19y = 17 \times (-2) + 19 \times 2 \\ &\iff 17(x + 2) + 19(y - 2) = 0 \end{aligned}$$

Si (x, y) est solution, alors 19 divise $x + 2$ en vertu du théorème de Gauss. Par conséquent, il existe $k \in \mathbb{Z}$ tel que $x = -2 + 19k$. Mais on a alors $y = 2 - 17k$. Réciproquement, on vérifie que tout couple de la forme $(-2 + 19k, 2 - 17k)$ est bien solution.

L'ensemble des solutions est donc

$$\{(-2 + 19k, 2 - 17k), k \in \mathbb{Z}\}$$

- On applique la méthode de résolution des équations diophantiennes du type $ax + by = c$.

Simplification par le pgcd Le pgcd de 323 et 391 est 17 (on le trouve en utilisant l'algorithme d'Euclide). L'équation est alors équivalente à $19x - 23y = 36$ avec 19 et 23 premiers entre eux.

Recherche d'une solution particulière Ici, on a clairement $-19 + 23 = 4$ donc $19 \times (-9) - 23 \times (-9) = 36$. Le couple $(-9, 9)$ est donc une solution particulière.

Recherche de la solution générale

$$\begin{aligned} 19x - 23y = 36 &\iff 19x - 23y = 19 \times (-9) - 23 \times (-9) \\ &\iff 19(x + 9) - 23(y + 9) = 0 \end{aligned}$$

Si (x, y) est solution, alors 23 divise $x + 9$ en vertu du théorème de Gauss. Par conséquent, il existe $k \in \mathbb{Z}$ tel que $x = -9 + 23k$. Mais on a alors $y = -9 + 19k$. Réciproquement, on vérifie que tout couple de la forme $(-9 + 23k, -9 + 19k)$ est bien solution.

L'ensemble des solutions est donc

$$\{(-9 + 23k, -9 + 19k), k \in \mathbb{Z}\}$$

- On applique la méthode de résolution des équations diophantiennes du type $ax + by = c$.

Simplification par le pgcd Le pgcd de 198 et 216 est 18 (on le trouve en utilisant l'algorithme d'Euclide). L'équation est alors équivalente à $11x - 12y = 2$ avec 11 et 12 premiers entre eux.

Recherche d'une solution particulière Ici, on a clairement $-11 + 12 = 1$ donc $11 \times (-2) + 12 \times 2 = 2$. Le couple $(-2, 2)$ est donc une solution particulière.

Recherche de la solution générale

$$\begin{aligned} 11x + 12y = 2 &\iff 11x + 12y = 11 \times (-2) + 12 \times 2 \\ &\iff 11(x + 2) + 12(y - 2) = 0 \end{aligned}$$

Si (x, y) est solution, alors 12 divise $x + 2$ en vertu du théorème de Gauss. Par conséquent, il existe $k \in \mathbb{Z}$ tel que $x = -2 + 12k$. Mais on a alors $y = 2 - 11k$. Réciproquement, on vérifie que tout couple de la forme $(-2 + 12k, 2 + 11k)$ est bien solution.

L'ensemble des solutions est donc

$$\{(-2 + 12k, 2 + 11k), k \in \mathbb{Z}\}$$

SOLUTION 21.

Remarquons qu'aucun des entiers x, y, z ne peut être égal à 1. De plus, on ne peut avoir $x > 3, y > 3$ et $z > 3$ car sinon $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} < 1$. Donc l'un des trois entiers est inférieur ou égal à 3. Supposons que ce soit x : on peut avoir $x = 2$ ou $x = 3$.

Cas $x = 2$: On a alors $\frac{1}{y} + \frac{1}{z} = \frac{1}{2}$. Comme auparavant, aucun des entiers y et z ne peut être égal à 2 et on ne peut avoir $y > 4$ et $z > 4$. L'un de ces deux entiers est donc inférieur ou égal à 4. Supposons que ce soit y .

Cas $y = 3$: On obtient $z = 6$.

Cas $y = 4$: On obtient $z = 4$.

Cas $x = 3$: On a alors $\frac{1}{y} + \frac{1}{z} = \frac{2}{3}$. On ne peut avoir $y > 3$ et $z > 3$. L'un de ces deux entiers est donc inférieur ou égal à 3. Supposons que ce soit y .

Cas $y = 2$: On obtient $z = 6$.

Cas $y = 3$: On obtient $z = 3$.

En conclusion, les solutions sont les triplets $(2, 3, 6)$, $(2, 4, 4)$, $(3, 3, 3)$ et toutes les permutations de ceux-ci.

SOLUTION 22.

Si (x, y) est un couple solution, alors $x(5x + 2y) = 3$ et donc x divise 3. Nécessairement $x \in \{\pm 1, \pm 3\}$.

► Si $x = 1$, alors l'équation devient $2 + 2y = 0$ i.e. $y = -1$.

► Si $x = -1$, alors l'équation devient $2 - 2y = 0$ i.e. $y = 1$.

► Si $x = 3$, alors l'équation devient $42 + 6y = 0$ i.e. $y = -7$.

► Si $x = -3$, alors l'équation devient $42 - 6y = 0$ i.e. $y = 7$.

Les couples solutions sont donc $(1, -1)$, $(-1, 1)$, $(3, -7)$, $(-3, 7)$.

SOLUTION 23.

Soit $(n, m) \in \mathbb{N}^2$ un éventuel couple vérifiant $n(n+1)(n+2) = m^2$.

Si n est pair, il existe $p \in \mathbb{N}$ tel que $n = 2p$. On en déduit que

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

Ainsi 2 divise m^2 et donc m puisque 2 est premier. Il existe donc $q \in \mathbb{N}$ tel que $m = 2q$. On en déduit que

$$p(2p+1)(p+1) = q^2$$

Or p , $2p+1$ et $p+1$ sont premiers entre eux deux à deux (il existe des relations de Bézout évidentes entre ces entiers) et on prouve alors classiquement que p , $2p+1$ et $p+1$ sont des carrés d'entiers en considérant les puissances de leurs facteurs premiers dans leurs décompositions en facteurs premiers. En particulier, il existe des entiers naturels c et d tels que $p = c^2$ et $p+1 = d^2$. Ainsi $d^2 - c^2 = 1$ i.e. $(d+c)(d-c) = 1$. On en déduit $d-c = d+c = 1$ et donc $c = 0$ et $d = 1$. Il s'ensuit que $n = 0$ puis $m = 0$.

Si n est impair, il existe $p \in \mathbb{N}$ tel que $n = 2p+1$. On en déduit que

$$2(2p+1)(p+1)(2p+3) = m^2$$

Ainsi 2 divise m^2 et donc m puisque 2 est premier. Il existe donc $q \in \mathbb{N}$ tel que $m = 2q$. On en déduit que

$$(2p+1)(p+1)(2p+3) = 2q^2$$

Donc 2 divise $(2p+1)(p+1)(2p+3)$. Comme $2p+1$ et $2p+3$ sont impairs, 2 divise $p+1$ et donc p est impair. Il existe donc $r \in \mathbb{N}$ tel que $p = 2r+1$. Il s'ensuit que

$$(4r+3)(r+1)(4r+5) = q^2$$

$r+1$ est premier avec $4r+3$ et $4r+5$ en vertu de relations de Bézout évidentes. De plus $(4r+5) - (4r+3) = 2$ donc le pgcd de $4r+3$ et $4r+5$ vaut 1 ou 2. Puisque $4r+3$ et $4r+5$ sont impairs, leur pgcd vaut 1 i.e. ces entiers sont premiers entre eux. Finalement, $r+1$, $4r+3$ et $4r+5$ sont premiers entre eux deux à deux et sont donc des carrés d'entiers comme précédemment. En particulier, il existe des entiers naturels c et d tels que $4r+3 = c^2$ et $4r+5 = d^2$. Ainsi $d^2 - c^2 = 2$ i.e. $(d+c)(d-c) = 2$. On en déduit que $d-c = 1$ et $d+c = 2$ i.e. $c = \frac{1}{2}$ et $d = \frac{3}{2}$ ce qui contredit le fait que c et d sont des entiers.

On en déduit finalement que la seule solution de l'équation $n(n+1)(n+2) = m^2$ est le couple $(0, 0)$.

SOLUTION 24.

1. a. Soit d un diviseur positif commun à α, β, c . Alors d divise $a = \alpha + c$, $b = \beta + c$ et c . Puisque a, b, c sont premiers entre eux dans leur ensemble, $d = 1$, ce qui prouve que α, β, c sont premiers entre eux dans leur ensemble. Puisque (a, b, c) est une solution de (E), on en déduit $c(a+b) = ab$ ou encore $\alpha\beta = c^2$. Soit d un diviseur commun à α et β . Alors d^2 divise $\alpha\beta = c^2$. On en déduit que d divise c et donc d est un diviseur commun à α, β, c . Puisque α, β, c sont premiers entre eux dans leur ensemble, $d = 1$, ce qui prouve que α et β sont premiers entre eux.

b. Remarquons tout d'abord que α et β sont des entiers naturels non nuls. En effet, puisque $\frac{1}{a} + \frac{1}{b} = \frac{1}{c}$, on a $\frac{1}{a} < \frac{1}{c}$ et $\frac{1}{b} < \frac{1}{c}$ puis $a > c$ et $b > c$. On va donc pouvoir considérer la décomposition en facteurs premiers de α et β . Soit p un nombre premier. Puisque $\alpha\beta = c^2$, $v_p(\alpha) + v_p(\beta) = 2v_p(c)$. Puisque α et β sont premiers entre eux, l'un au moins des deux entiers $v_p(\alpha)$ et $v_p(\beta)$ est nul. L'autre est donc nécessairement pair. Finalement, les deux entiers $v_p(\alpha)$ et $v_p(\beta)$ sont pairs puisque 0 est pair. Ainsi toutes les valuations apparaissant dans la décomposition en facteurs premiers de α et β sont paires, ce qui prouve que α et β sont des carrés. Il existe donc des entiers naturels non nuls u et v tels que $\alpha = u^2$ et $\beta = v^2$. Alors $c^2 = \alpha\beta = u^2v^2$ donc $c = uv$. Ainsi $a = \alpha + c = (u+v)u$ et $b = \beta + c = (u+v)v$.
2. Soit $(a, b, c) \in (d\mathbb{N}^*)^3$ une solution de (E). Alors en posant $d = a \wedge b \wedge c$, $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ et $c' = \frac{c}{d}$ sont premiers entre eux dans leur ensemble. Ce qui précède assure l'existence d'un couple $(u, v) \in (\mathbb{N}^*)^2$ tel que $a' = (u+v)u$, $b' = (u+v)v$ et $c' = uv$. On a donc $a = d(u+v)u$, $b = d(u+v)v$ et $c = d uv$. Réciproquement, soit $(d, u, v) \in (\mathbb{N}^*)^3$ et posons $a = d(u+v)u$, $b = d(u+v)v$ et $c = d uv$. Alors

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{d(u+v)u} + \frac{1}{d(u+v)v} = \frac{v+u}{d(u+v)uv} = \frac{1}{d uv} = \frac{1}{c}$$

donc (a, b, c) est solution de (E).

Finalement les solutions de (E) sont les triples de la forme $(d(u+v)u, d(u+v)v, d uv)$ où $(d, u, v) \in (\mathbb{N}^*)^3$.

SOLUTION 25.

Soit $(n, m) \in \mathbb{N}^2$ une éventuelle solution. Alors $2^n = m^3 - 1 = (m-1)(m^2 + m + 1)$. Puisque 2 est premier, $m-1$ et $m^2 + m + 1$ sont des puissances de 2. Or $m^2 + m + 1 = m(m+1) + 1$ est impair puisque $m(m+1)$ est pair. Or la seule puissance de 2 impaire est $2^0 = 1$ donc $m^2 + m + 1 = 1$ i.e. $m = 0$ (on ne peut avoir $m = -1$ car $m \in \mathbb{N}$). Il vient alors $2^n = -1$, ce qui est absurde. L'équation $2^n + 1 = m^3$ d'inconnue $(n, m) \in \mathbb{N}^2$ n'admet donc pas de solution.

SOLUTION 26.

1.

$$\begin{cases} x \wedge y = 3 \\ x \vee y = 135 \end{cases} \iff \exists (x', y') \in \mathbb{Z}^2, \begin{cases} x = 3x', y = 3y' \\ x' \wedge y' = 1 \\ x'y' = 45 \end{cases}$$

Les couples (x', y') possibles sont $(1, 45)$, $(5, 9)$, $(9, 5)$ et $(45, 1)$. Ainsi les solutions sont $(3, 135)$, $(15, 27)$, $(27, 15)$ et $(135, 3)$.

2.

$$\begin{cases} x + y = 100 \\ x \wedge y = 10 \end{cases} \iff \exists (x', y') \in \mathbb{Z}^2, \begin{cases} x = 10x', y = 10y' \\ x' \wedge y' = 1 \\ x' + y' = 10 \end{cases}$$

Les couples (x', y') possibles sont $(1, 9)$, $(3, 7)$, $(7, 3)$ et $(9, 1)$. Ainsi les solutions sont $(10, 90)$, $(30, 70)$, $(70, 30)$ et $(90, 10)$.

SOLUTION 27.

1. On raisonne par récurrence.

Initialisation On a $F_0 F_2 - F_1^2 = -1 = (-1)^1$ donc la formule est vraie au rang 1.

Hérédité Supposons que $F_{n-1} F_{n+1} - F_n^2 = (-1)^n$ pour un certain $n \in \mathbb{N}^*$.

$$\begin{aligned} F_n F_{n+2} - F_{n+1}^2 &= F_n (F_{n+1} + F_n) - F_{n+1} (F_{n-1} + F_n) \\ &= F_n^2 - F_{n+1} F_{n-1} = -(-1)^n = (-1)^{n+1} \end{aligned}$$

La formule est donc également vraie au rang $n+1$.

Conclusion La formule est vraie pour tout $n \in \mathbb{N}^*$.

On a donc une relation de Bézout entre F_n et F_{n-1} : ces deux entiers sont donc premiers entre eux.

2. On raisonne par récurrence sur n (et pas sur p). L'hypothèse de récurrence au rang $n \in \mathbb{N}$ est la suivante :

(H_n) : Pour tout $p \in \mathbb{N}^*$, $F_{n+p} = F_p F_{n+1} + F_{p-1} F_n$.

Initialisation On a pour tout $p \in \mathbb{N}^*$:

$$F_p F_1 + F_{p-1} F_0 = F_p$$

donc (H_0) est vraie.

Hérédité Supposons (H_n) pour un certain $n \in \mathbb{N}$. Soit $p \in \mathbb{N}^*$. Remarquons que $F_{(n+1)+p} = F_{n+(p+1)}$. Or $p+1 \in \mathbb{N}^*$. On applique notre hypothèse de récurrence (H_n) :

$$\begin{aligned} F_{n+(p+1)} &= F_{p+1} F_{n+1} + F_p F_n \\ &= (F_p + F_{p-1}) F_{n+1} + F_p F_n \\ &= F_p (F_{n+1} + F_n) + F_{p-1} F_{n+1} \\ &= F_p F_{n+2} + F_{p-1} F_{n+1} \end{aligned}$$

Ceci étant vrai quelque soit le choix de p , on en déduit que (H_{n+1}) est vraie.

Conclusion Pour tout $n \in \mathbb{N}$, (H_n) est vraie.

Soit $(n, p) \in \mathbb{N} \times \mathbb{N}^*$.

- Soit d un diviseur commun de F_n et F_p . Comme $F_{n+p} = F_p F_{n+1} + F_{p-1} F_n$, d divise également F_{n+p} . Donc d est un diviseur commun de F_p et F_{n+p} .
- Réciproquement, soit d un diviseur commun de F_p et F_{n+p} . On en déduit que d divise $F_{p-1} F_n$. Or F_p et F_{p-1} sont premiers entre eux et d divise F_p , donc d et F_{p-1} sont également premiers entre eux. D'après le théorème de Gauss, d divise F_n . C'est donc un diviseur commun de F_n et F_p .

On en conclut que $F_n \wedge F_p = F_{n+p} \wedge F_p$.

3. Soit $(m, n) \in \mathbb{N}^2$. On effectue la division euclidienne de m par n : $m = nq + r$. En itérant le résultat de la question précédente, on a

$$F_n \wedge F_r = F_n \wedge F_{r+n} = F_n \wedge F_{r+2n} = \dots = F_n \wedge F_{r+nq} = F_n \wedge F_m$$

On conclut grâce à l'algorithme d'Euclide. Soit $d = m \wedge n$. Notons $a_0, \dots, a_m = d$ la suite des restes non nuls obtenus par l'algorithme d'Euclide. D'après ce qui précède,

$$F_m \wedge F_n = F_n \wedge F_{a_0} = F_{a_0} \wedge F_{a_1} = \dots = F_{a_m} \wedge F_0 = F_d$$

SOLUTION 28.

Soit d un diviseur commun à a et bc . Par conséquent d divise bc . Mais d divise a qui est premier avec b . Donc d est premier avec b . Par le théorème de Gauss, d divise donc c . Finalement, d est un diviseur commun à a et c .

Réciproquement, soit d un diviseur commun à a et c . Il est alors évident que d est aussi un diviseur commun de a et bc .

On conclut donc que $a \wedge bc = a \wedge c$.

SOLUTION 29.

Il existe $(a', b') \in \mathbb{Z}^2$ tels que $a = da'$ et $b = db'$ et $a' \wedge b' = 1$. On a alors $m = da'b'$ puis

$$(a + b) \wedge m = d[(a' + b') \wedge a'b'].$$

Nous allons montrer que $(a' + b') \wedge a'b' = 1$. Supposons par l'absurde que $a'b'$ et $a' + b'$ admettent un diviseur premier commun p . Comme a' et b' sont premiers entre eux, $p|a'b'$ implique soit $p|a'$ soit $p|b'$. Quitte à changer leurs rôles on peut supposer que $p|a'$. Comme d'autre part $p|a' + b'$, on déduit que $p|b'$. Ainsi p est un diviseur premier commun de a' et b' , ce qui contredit que $a' \wedge b' = 1$. Ainsi $(a' + b') \wedge a'b' = 1$ et finalement $(a + b) \wedge m = d$.

REMARQUE. On peut également se passer du lemme d'Euclide et utiliser le théorème de Bezout pour montrer que $(a' + b') \wedge a'b' = 1$. Comme $a' \wedge b' = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $a'u + b'v = 1$. En élevant au carré, on obtient $a'^2 u^2 + b'^2 v^2 + 2a'b'uv = 1$. Or $a'^2 = a'(a' + b') - a'b'$ et $b'^2 = b'(a' + b') - a'b'$ de sorte que

$$(a' + b')(a'u^2 + b'v^2 + a'b'(2uv - u^2 - v^2)) = 1$$

Cette relation de Bezout permet d'affirmer que $(a' + b') \wedge a'b' = 1$. ■

SOLUTION 30.

Par un changement d'indice

$$\begin{aligned} 2 \sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor &= \sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor + \sum_{k=1}^{b-1} \left\lfloor \frac{(b-k)a}{b} \right\rfloor \\ &= \sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor + \left\lfloor a - \frac{ka}{b} \right\rfloor \end{aligned}$$

- Si $\frac{ka}{b}$ est entier, alors

$$\left\lfloor \frac{ka}{b} \right\rfloor + \left\lfloor a - \frac{ka}{b} \right\rfloor = a$$

- Sinon

$$\left\lfloor \frac{ka}{b} \right\rfloor + \left\lfloor a - \frac{ka}{b} \right\rfloor = a - 1$$

Il reste donc à trouver le nombre d'entier $k \in \llbracket 1, b-1 \rrbracket$ tel que $\frac{ka}{b}$ soit entier.

Posons $d = a \wedge b$, $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ de sorte que $a' \wedge b' = 1$. Soit $k \in \llbracket 1, b-1 \rrbracket$. Alors $\frac{ka}{b} = \frac{ka'}{b'}$. Ainsi $\frac{ka}{b}$ est entier si et seulement si k est un multiple de b' . Or il existe exactement $d-1$ multiples de b' compris entre 1 et $b-1$. Il s'ensuit que

$$2 \sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor = (d-1)a + ((b-1) - (d-1))(a-1) = ab - a - b + d$$

On en déduit l'inégalité voulue.

SOLUTION 31.

Supposons les a_i premiers entre eux à deux. On suppose que les b_i possèdent un diviseur premier commun p . Notamment p divise b_1 donc il existe $j \in \llbracket 2, r \rrbracket$ tel que p divise a_j d'après le lemme d'Euclide. Mais p divise également b_j donc il existe $k \in \llbracket 1, r \rrbracket \setminus \{j\}$ tel que p divise a_k toujours d'après le lemme d'Euclide. Ainsi p divise a_j et a_k et $k \neq j$. Puisque $a_j \wedge a_k = 1$, a_j et a_k n'ont pas de diviseur premier commun d'où une contradiction. Ainsi les b_i ne possèdent pas de diviseur premier commun : il sont donc premiers entre eux dans leur ensemble.

Supposons maintenant les b_i premiers entre eux dans leur ensemble. Soit $(j, k) \in \llbracket 1, r \rrbracket^2$ tel que $j \neq k$. Posons $d = a_j \wedge a_k$. Puisque d divise a_j , d divise b_i pour tout $i \in \llbracket 1, r \rrbracket \setminus \{j\}$. De même, d divise a_k donc d divise b_i pour tout $i \in \llbracket 1, r \rrbracket \setminus \{k\}$. Finalement, d divise tous les b_i et donc leur pgcd, à savoir 1. Ainsi $d = 1$ et a_j et a_k sont premiers entre eux.

SOLUTION 32.

1. Soient m et n deux entiers premiers entre eux. Si d_1 est un diviseur de m et d_2 est un diviseur de n , $d_1 d_2$ est un diviseur de mn . Réciproquement, soit d un diviseur de mn . Posons

$$d_1 = d \wedge m \text{ et } d_2 = d \wedge n.$$

d_1 et d_2 sont respectivement des diviseurs de m et n qui sont premiers entre eux : ils sont donc aussi premiers entre eux. De plus, d_1 et d_2 divisent d donc $d_1 d_2$ divise d . On écrit les relations de Bezout suivantes

$$d_1 = u_1 d + v_1 m \text{ et } d_2 = u_2 d + v_2 n$$

Par conséquent,

$$d_1 d_2 = v_1 v_2 mn + (u_1 u_2 d + v_1 m u_2 + v_2 n u_1) d$$

Comme d divise mn , d divise $d_1 d_2$ et finalement, $d = d_1 d_2$.

Les diviseurs de mn sont exactement les produits d'un diviseur de m et d'un diviseur de n . Montrons que ces produits sont tous distincts. Soient d_1 et d'_1 des diviseurs de m , d_2 et d'_2 des diviseurs de n tels que $d_1 d_2 = d'_1 d'_2$. Comme m et n sont premiers entre eux, d_1 et d'_2 sont premiers entre eux. Donc d_1 divise d'_1 . De la même manière, d'_1 divise d_1 donc $d_1 = d'_1$ et $d_2 = d'_2$.

$$\begin{aligned} S(mn) &= \sum_{d|mn} d = \sum_{d_1|m, d_2|n} d_1 d_2 \\ &= \left(\sum_{d_1|m} d_1 \right) \left(\sum_{d_2|n} d_2 \right) = S(m)S(n) \end{aligned}$$

2. a. Soit d un diviseur de p . Il existe donc $k \in \mathbb{N}$ tel que $p = kd$.

$$2^p - 1 = 2^{kd} - 1 = (2^d)^k - 1 = (2^d - 1) \sum_{l=0}^{k-1} 2^{ld}$$

Or $2^p - 1$ est premier donc $2^d - 1$ vaut 1 ou $2^p - 1$ et d vaut 1 ou p , ce qui prouve que p est premier.

- b. En utilisant la première question,

$$S(n) = S(2^{p-1})S(2^p - 1)$$

car la relation de Bezout $2 \times 2^{p-1} - (2^p - 1) = 1$ prouve que 2^{p-1} et $2^p - 1$ sont premiers entre eux.

Les diviseurs de 2^{p-1} sont les 2^k avec $0 \leq k \leq p-1$ donc

$$S(2^{p-1}) = \sum_{k=0}^{p-1} 2^k = 2^p - 1$$

De plus, $2^p - 1$ est premier par hypothèse donc ses seuls diviseurs sont 1 et lui-même donc

$$S(2^p - 1) = 1 + 2^p - 1 = 2^p$$

Finalement on a bien $S(n) = 2^p(2^p - 1) = 2n$.

3. Soit n un nombre parfait pair. Notons $p-1$ l'exposant de 2 dans la décomposition de n en facteurs premiers. Ainsi $n = 2^{p-1}m$ où m est impair. Comme n est pair, $p \geq 2$. De plus, $S(n) = S(2^{p-1})S(m)$ car m et 2 sont premiers entre eux. Or $S(n) = 2n = 2^p m$ par hypothèse et $S(2^{p-1}) = 2^p - 1$. Ainsi $2^p m = (2^p - 1)S(m)$. Comme $2^p - 1$ et 2^p sont premiers entre eux, 2^{p-1} divise m et 2^p divise $S(m)$. Il existe donc $k \in \mathbb{N}^*$ tel que $m = (2^p - 1)k$ et $S(m) = 2^p k$. Comme $p \geq 2$, $2^p - 1 \neq 1$. Ainsi k et $m = (2^p - 1)k$ sont des diviseurs de m distincts. Donc $S(m) \geq k + (2^p - 1)k = 2^p k$. Or $S(m) = 2^p k$ donc k et $m = (2^p - 1)k$ sont les seuls diviseurs de m . Ceci prouve que m est premier et que k vaut 1. Ainsi $m = 2^p - 1$ et p est premier d'après une question précédente.

SOLUTION 33.

1. On peut écrire m sous la forme $2^n k$ où k est impair donc de la forme $2l + 1$. Remarquons que

$$X^{2l+1} + 1 = (X + 1) \sum_{i=0}^{2l} (-1)^i X^i.$$

En spécialisant cette relation pour $X = 2^m$, on obtient :

$$2^m + 1 = (2^{2^n})^{2l+1} + 1 = (2^{2^n} + 1) \sum_{i=0}^{2l} (-1)^i (2^{2^n})^i.$$

Ainsi $2^{2^n} + 1$ est un diviseur de $2^m + 1$ distinct de 1 car $k \geq 1$ et de $2^m + 1$ si $k \neq 1$. C'est donc que $k = 1$ et m est bien de la forme 2^n . On pouvait également remarquer que $2^{2^n} \equiv -1[2^{2^n} + 1]$ et donc $2^{2^n k} \equiv -1[2^{2^n} + 1]$ car k est impair. Ainsi $2^m + 1 \equiv 0[2^{2^n} + 1]$ i.e. $2^{2^n} + 1$ divise $2^m + 1$. Puisque $2^m + 1$ est premier, $2^{2^n} + 1 = 1$ ou $2^{2^n} + 1 = 2^m + 1$. Le premier cas est impossible : c'est donc que $2^{2^n} + 1 = 2^m + 1$, ce qui implique $m = 2^n$.

2. On peut supposer $m > n$.

$$\begin{aligned}
 F_m &= 2^{2^m} + 1 + \sum_{k=1}^{2^{m-n}} (-1)^k 2^{2^m - k 2^n} \\
 &\quad - \sum_{k=1}^{2^{m-n}} (-1)^k 2^{2^m - k 2^n} \\
 &= 2 + \sum_{k=0}^{2^{m-n}-1} (-1)^k 2^{2^m - k 2^n} \\
 &\quad + \sum_{k=1}^{2^{m-n}} (-1)^{k-1} 2^{2^m - k 2^n} \\
 &= 2 + \sum_{k=0}^{2^{m-n}-1} (-1)^k 2^{2^n} 2^{2^m - (k+1)2^n} \\
 &\quad + \sum_{k=1}^{2^{m-n}} (-1)^{k-1} 2^{2^m - k 2^n} \\
 &= 2 + \sum_{k=1}^{2^{m-n}} (-1)^{k-1} 2^{2^n} 2^{2^m - k 2^n} \\
 &\quad + \sum_{k=1}^{2^{m-n}} (-1)^{k-1} 2^{2^m - k 2^n} \\
 &= 2 + \sum_{k=1}^{2^{m-n}} (-1)^{k-1} (2^{2^n} + 1) 2^{2^m - k 2^n} \\
 &= 2 + F_n \sum_{k=1}^{2^{m-n}} (-1)^{k-1} 2^{2^m - k 2^n}
 \end{aligned}$$

Ainsi $F_m \wedge F_n$ divise 2. Comme F_n et F_m sont impairs, $F_m \wedge F_n = 1$.

A nouveau, on pouvait raisonner par congruences. En effet, $2^{2^n} \equiv -1[F_n]$. En élevant à la puissance 2^{m-n} , on obtient $2^{2^m} \equiv 1[F_n]$ car 2^{m-n} est pair ($m > n$). Il s'ensuit que $F_m \equiv 2[F_n]$. Par conséquent, $F_m \wedge F_n$ divise 2. Comme F_m est pair, $F_m \wedge F_n = 1$.

SOLUTION 34.

1. Soit $k \in \llbracket 1, p-1 \rrbracket$. On sait que $k \binom{p}{k} = p \binom{p-1}{k-1}$. Donc p divise $k \binom{p}{k}$. Comme p est premier et que $1 \leq k \leq p-1$, k et p sont premiers entre eux. Par conséquent, p divise $\binom{p}{k}$ en vertu du théorème de Gauss.
2. On démontre le résultat par récurrence sur n .

Initialisation $0^p - 0 = 0$ est clairement divisible par p .

Hérédité Supposons que $n^p - n$ soit divisible par n pour un certain $n \in \mathbb{N}$. Alors

$$\begin{aligned}
 (n+1)^p - (n+1) &= \left(\sum_{k=0}^p \binom{p}{k} n^k \right) - (n+1) \\
 &= n^p - n + \sum_{k=1}^{p-1} \binom{p}{k} n^k
 \end{aligned}$$

Tous les termes de la somme sont divisibles par p d'après la question précédente et $n^p - n$ l'est également d'après l'hypothèse de récurrence. Donc $(n+1)^p - (n+1)$ est aussi divisible par p .

Conclusion Pour tout entier $n \in \mathbb{N}$, $n^p - n$ est divisible par p (i.e. $n^p \equiv n[p]$).

SOLUTION 35.

1. $a^r - 1$ est divisible par $a - 1$. Comme $a^r - 1$ est premier, on a deux possibilités :

- $a - 1 = 1$ i.e. $a = 2$,
- $a - 1 = a^r - 1$ ce qui entraîne $a = 1$ ou $r = 1$, ce qui est contraire aux hypothèses.

Si $r = pq$ avec $p \neq 1$ et $p \neq r$, alors $2^r - 1 = (2^p)^q - 1$ est divisible par $2^p - 1$. De plus, $2^p - 1 \neq 1$ et $2^p - 1 \neq 2^r - 1$, ce qui contredit la primalité de $2^r - 1$. Par conséquent, r est premier.

2. La réciproque est fausse puisque $2^{11} - 1 = 23 \times 89$.

SOLUTION 36.

1. a. Il existe donc $b \in \mathbb{N}^*$ tel que $n = ab$. On factorise $2^n - 1$ de la manière suivante :

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1) \sum_{k=0}^{b-1} 2^{ka}$$

Ainsi $2^a - 1$ divise M_n .

On peut également remarquer que $2^a \equiv 1[2^a - 1]$ donc $2^{ab} \equiv 1[2^a - 1]$. Ainsi $2^a - 1$ divise M_n .

b. On suppose M_n premier. Soit a un diviseur positif de n . La question précédente montre que $2^a - 1$ divise M_n . M_n étant premier, on a donc $2^a - 1 = 1$ i.e. $a = 1$ ou $2^a - 1 = 2^n - 1$ i.e. $a = n$. Les seuls diviseurs positifs de n sont donc 1 et n , ce qui prouve que n est premier.

2. a. $M_p = 2 \times 2^{p-1} - 1$. Comme $p - 1 \geq 0$, M_p est impair. Donc q est impair. Ainsi $2 \wedge q = 1$. En appliquant le petit théorème de Fermat, on a donc $2^q \equiv 2[q]$. Ainsi q divise $2^q - 2 = 2(2^{q-1} - 1)$. Comme q est impair $q \wedge 2 = 1$ et donc q divise $2^{q-1} - 1$ i.e. $2^{q-1} \equiv 1[q]$.

b. A est une partie non vide de \mathbb{N} puisque $q - 1 \in A$. A admet donc un minimum.

c. Soit r le reste de la division euclidienne de p par m . Comme $2^p \equiv 1[q]$ et $2^m \equiv 1[q]$, $2^r \equiv 1[q]$. Or $0 \leq r < m$ et $m = \min A$. C'est donc que $r = 0$. Ainsi m divise p . Comme p est premier, on a donc $m = 1$ ou $m = p$. Puisque $2^1 \not\equiv 1[q]$, c'est donc que $m = p$.

d. Notons à nouveau r le reste de la division euclidienne de $q - 1$ par p . Comme $2^{q-1} \equiv 1[p]$ et $2^p \equiv 1[p]$, $2^r \equiv 1[p]$. Or $0 \leq r < p$ et $p = \min A$. C'est donc que $r = 0$. Ainsi p divise $q - 1$ i.e. $q \equiv 1[p]$.

e. Comme q est impair, $q - 1$ est pair i.e. 2 divise $q - 1$. On vient de voir que p divise également $q - 1$. p étant impair, 2 et p sont premiers entre eux et donc $2p$ divise $q - 1$ i.e. $q \equiv 1[2p]$.

3. Si $n = 1$, on a évidemment $n \equiv 1[2p]$. Sinon n peut s'écrire sous la forme $n = \prod_{i=1}^r q_i$ où les q_i sont des nombres premiers. Soit $i \in \llbracket 1, r \rrbracket$. q_i divise n et donc M_p . La question précédente montre que $q_i \equiv 1[2p]$. En multipliant membre à membre ces congruences, on obtient $n \equiv 1[2p]$.

SOLUTION 37.

Soient p et q deux nombres premiers consécutifs avec $p < q$.

Si $p = 2$, alors $q = 3$ et $p + q = 5$ ne peut être le produit de deux nombres premiers.

Si $p > 2$, alors p et q sont impairs donc $p + q$ est pair. Supposons qu'il existe deux nombres premiers a et b tels que $p + q = ab$. Comme $p + q$ est pair, un des deux nombres premiers a et b est égal à 2 par unicité de la décomposition en facteurs premiers. Supposons sans perte de généralité que $a = 2$. Alors $b = \frac{p+q}{2}$ est un nombre premier strictement compris entre p et q , ce qui contredit le fait que p et q sont des nombres premiers consécutifs.

SOLUTION 38.

Il existe $c \in \mathbb{N}^*$ tel que $ab = c^n$.

Soit p un nombre premier. Alors $v_p(ab) = v_p(c^n)$ i.e. $v_p(a) + v_p(b) = n v_p(c)$. Puisque $a \wedge b = 1$, p ne peut être un facteur commun de a et b : on a donc $v_p(a) = 0$ ou $v_p(b) = 0$. Dans les deux cas, $v_p(a)$ et $v_p(b)$ sont des multiples de n .

Il existe donc deux familles d'entiers naturels presque nulles $(\alpha_p)_{p \in \mathcal{P}}$ et $(\beta_p)_{p \in \mathcal{P}}$ telles que pour tout $p \in \mathcal{P}$, $v_p(a) = n\alpha_p$ et $v_p(b) = n\beta_p$. On a alors

$$a = \prod_{p \in \mathcal{P}} p^{n\alpha_p} = \left(\prod_{p \in \mathcal{P}} p^{\alpha_p} \right)^n \quad \text{et} \quad b = \prod_{p \in \mathcal{P}} p^{n\beta_p} = \left(\prod_{p \in \mathcal{P}} p^{\beta_p} \right)^n$$

Ainsi a et b sont des puissances $n^{\text{èmes}}$ d'entiers.

SOLUTION 39.

1. On a $n = 2k + 1$ pour un certain $k \in \mathbb{Z}$. Ainsi $n^2 = (2k + 1)^2 = 4k(k + 1) + 1$. L'un des deux nombres k ou $k + 1$ est un multiple de 2, ce qui entraîne que $4k(k + 1)$ est un multiple de 8, donc $n^2 \equiv 1 \pmod{8}$.
2. D'après la question précédente on sait déjà que $p^2 \equiv 1 \pmod{8}$. Comme p n'est pas divisible par 3 on a $p \equiv \pm 1 \pmod{3}$, donc $p^2 \equiv 1 \pmod{3}$. Ainsi 8 et 3 divisent $p^2 - 1$, et donc PPCM(8, 3) = 24 divise aussi $p^2 - 1$.

SOLUTION 40.

A l'aide de MAPLE par exemple, on constate que u_1 se termine par deux chiffres 9, u_2 par quatre chiffres 9, u_3 par huit chiffres 9... On fait alors la conjecture que u_n se termine par 2^n chiffres 9. On utilise alors la remarque suivante : l'écriture décimale d'un entier N se termine au moins par p chiffres 9 si et seulement si $N + 1$ est divisible par 10^p (en effet, $\sum_{k=0}^{p-1} 9 \cdot 10^k = 10^p - 1$). Soit donc HR(n) l'hypothèse

de récurrence $u_n + 1$ est divisible par 10^{2^n} .

HR(0) est clairement vraie. Supposons HR(n) pour un certain $n \in \mathbb{N}$. Il existe donc $p \in \mathbb{N}$ tel que $u_n = -1 + 10^{2^n} p$. On a alors après développement et simplification

$$\begin{aligned} u_{n+1} &= -1 + 6(10^{2^n} p)^2 - 8(10^{2^n} p)^3 + 3(10^{2^n} p)^4 \\ &= -1 + 6 \cdot 10^{2^{n+1}} p^2 - 8 \cdot 10^{3 \cdot 2^n} p^3 + 3 \cdot 10^{2^{n+2}} p^4 \\ &= -1 + 10^{2^{n+1}} (6p^2 - 8 \cdot 10^{2^n} p^3 + 3 \cdot 10^{2^{n+1}} p^4) \end{aligned}$$

Ainsi $10^{2^{n+1}}$ divise $u_{n+1} + 1$ et HR($n + 1$) est vraie.

Par conséquent HR(n) est vraie pour tout $n \in \mathbb{N}$. Notamment pour $n = 11$, on peut affirmer que l'écriture décimale de u_{11} se termine par au moins 2^{11} chiffres 9. Or $2^{11} = 2048 > 2010$.

SOLUTION 41.

Avec le programme de première année :

Pour $k \in \llbracket 1, n \rrbracket$, notons r_k le reste de la division euclidienne de $\sum_{j=1}^k x_j$ par n . Si un des restes est nul, c'est terminé. Sinon, ces n restes

sont dans l'ensemble $\llbracket 1, n-1 \rrbracket$ qui est de cardinal $n-1$ donc deux des restes sont égaux. Il existe donc $(k, l) \in \llbracket 1, n \rrbracket^2$ tel que $k < l$ et $r_k = r_l$. Mais alors $\sum_{j=1}^l x_j - \sum_{j=1}^k x_j = \sum_{j=l+1}^k x_j$ est divisible par n .

Avec le programme de seconde année :

Pour $k \in \llbracket 1, n \rrbracket$, notons c_k la classe de $\sum_{j=1}^k x_j$ modulo n . Si une des classes est nulle, c'est terminé. Sinon, ces n classes sont dans $\mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}$ qui est de cardinal $n-1$ donc deux des classes sont égales. Il existe donc $(k, l) \in \llbracket 1, n \rrbracket^2$ tel que $k < l$ et $c_k = c_l$. Mais alors $\sum_{j=1}^l x_j - \sum_{j=1}^k x_j = \sum_{j=l+1}^k x_j$ est divisible par n .

SOLUTION 42.

Soit $(a_0, \dots, a_{n-1}) \in \llbracket 0, b-1 \rrbracket^n$. Alors

$$0 \leq \sum_{k=0}^{n-1} a_k b^k \leq \sum_{k=0}^{n-1} (b-1) b^k = b^n - 1$$

Ceci prouve que φ est bien définie.

Puisque $\text{card}(\llbracket 0, b-1 \rrbracket^n) = \text{card}(\llbracket 0, b^n-1 \rrbracket) = b^n$, il suffit de montrer l'injectivité ou la surjectivité de φ pour établir sa bijectivité. Montrons par exemple l'injectivité de φ .

Soient (a_0, \dots, a_{n-1}) et (c_0, \dots, c_{n-1}) deux n -uplets distincts de $\llbracket 0, b-1 \rrbracket^n$. Notons j le plus grand indice tel que $a_j \neq c_j$. Alors

$$\begin{aligned} |\varphi(a_0, \dots, a_{n-1}) - \varphi(c_0, \dots, c_{n-1})| &= \left| \sum_{k=0}^j a_k b^k - \sum_{k=0}^j c_k b^k \right| \\ &\geq |a_j - c_j| b^j - \left| \sum_{k=0}^{j-1} (a_k - c_k) b^k \right| \\ &\geq |a_j - c_j| b^j - \sum_{k=0}^{j-1} |a_k - c_k| b^k \text{ par inégalité triangulaire} \end{aligned}$$

Or $a_j - c_j$ est un entier non nul donc $|a_j - c_j| \geq 1$. De plus, $|a_k - c_k| \leq b-1$ pour tout $k \in \llbracket 0, j-1 \rrbracket$. Il s'ensuit que

$$|\varphi(a_0, \dots, a_{n-1}) - \varphi(c_0, \dots, c_{n-1})| \geq b^j - \sum_{k=0}^{j-1} (b-1) b^k = 1$$

En particulier, $\varphi(a_0, \dots, a_{n-1}) \neq \varphi(c_0, \dots, c_{n-1})$, ce qui prouve l'injectivité de φ et, par suite, sa bijectivité.

SOLUTION 43.

Soient a et b tels que $(aabb)_{10}$ soit un carré d'entier. Autrement dit il existe $n \in \mathbb{N}$ tel que $1100a + 11b = n^2$. Mais $1100a + 11b = 11(100a + b)$ donc 11 divise n^2 et donc n puisque 11 est premier. On en déduit que 11 divise $100a + b$. Autrement dit $100a + b \equiv 0[11]$. Mais $100 \equiv 1[11]$ donc $a + b \equiv 0[11]$. Mais a et b sont des chiffres donc appartiennent à $\llbracket 0, 9 \rrbracket$. On a donc $a + b = 0$ ou $a + b = 11$.

Si $a + b = 0$, alors $a = b = 0$ et 0 est bien un carré d'entier.

Si $a + b = 11$, alors il faut explorer les différents cas en tenant compte du fait que a et b appartiennent à $\llbracket 0, 9 \rrbracket$.

- Si $a = 2$ et $b = 9$, 2299 n'est pas un carré d'entier.
- Si $a = 3$ et $b = 8$, 3388 n'est pas un carré d'entier.
- Si $a = 4$ et $b = 7$, 4477 n'est pas un carré d'entier.
- Si $a = 5$ et $b = 6$, 5566 n'est pas un carré d'entier.
- Si $a = 6$ et $b = 5$, 6655 n'est pas un carré d'entier.
- Si $a = 7$ et $b = 4$, 7744 est un carré d'entier.
- Si $a = 8$ et $b = 3$, 8833 n'est pas un carré d'entier.

- Si $a = 9$ et $b = 2$, 9922 n'est pas un carré d'entier.

Finalement, les deux seuls nombres s'écrivant en base 10 sous la forme $(aabb)_{10}$ sont 0 et 7744.