1 ★★ Montrer que $5^{20} + 2^{30}$ n'est pas un nombre premier.

Corrigé : On va proposer deux méthodes.

• La première technique se base sur des identités remarquables :

$$5^{20} + 2^{30} = (5^{10} + 2^{15})^2 - 2 \times 5^{10} \times 2^{15} = ((5^{10} + 2^{15}) + 5^5 \times 2^8)((5^{10} + 2^{15}) - 5^5 \times 2^8)$$

Il reste à démontrer que cette factorisation est non triviale. Il est clair que le premier facteur est différent de 1. Pour le second facteur, on a :

$$5^{10} + 2^{15} - 5^5 \times 2^8 = 5^{10} + 2^{15} - 5^5 \times 4^4 > 5^{10} + 2^{15} - 5^5 \times 5^4 = (5^{10} - 5^9) + 2^{15} > 1$$

Ce qui démontre que ce nombre est composé.

• On peut aussi raisonner modulo 13. On trouve $5^4 \equiv 1$ [13] et $2^6 \equiv -1$ [13]. On en déduit que :

$$5^{20} + 2^{30} = (5^4)^5 + (2^6)^5 \equiv 1^5 + (-1)^5 \equiv 0 \text{ [13]}$$

Ce nombre est divisible par 13 donc il n'est pas premier.

$$\boxed{5^{20} + 2^{30} \text{ n'est pas premier}}$$

2 Trouver tous les $(x, y) \in \mathbb{Z}^2$ tels que : $5x + 7y = 8$.

Corrigé : On a $\text{pgcd}(5, 7) = 1$ et $1|8$, on sait que l'équation a des solutions. On trouve directement les coefficients de Bézout ou on utilise l'algorithme d'Euclide pour trouver :

$$5 \times 3 + 7 \times (-2) = 1$$

en multipliant par 8, il vient :

$$5 \times 24 + 7 \times (-16) = 8$$

Le couple $(24, -16)$ est une solution particulière de l'équation. En utilisant la méthode de l'exercice 61, on en déduit que les solutions sont de la forme :

$$x = 24 + 7k \text{ et } y = -16 - 5k \text{ avec } k \in \mathbb{Z}$$

$$\boxed{\mathcal{S} = \{(24 + 7k, -16 - 5k),\ k \in \mathbb{Z}\}}$$

Il était également possible de résoudre cette équation en utilisant une congruence module 5 *(pour avoir une équation en* y*) ou modulo* 7 *(pour avoir une équation en* x*).*

3 ★★ Trouver tous les $(x, y, z) \in \mathbb{Z}^3$ tels que : $18x + 20y + 15z = 1$.

Corrigé : Les entiers 18, 20 et 15 sont premiers entre eux, l'équation a donc des solutions.

• **Analyse.** On se donne $(x, y, z) \in \mathbb{Z}^3$ une solution de l'équation. On passe modulo 2 pour se ramener a une équation avec une inconnue :

$$15z \equiv z \equiv 1 \text{ [2]} \Leftrightarrow \exists k \in \mathbb{Z},\ z = 1 + 2k$$

On reporte dans l'équation pour obtenir :

$$18x + 20y + 15(1 + 2k) = 1 \Leftrightarrow 9x + 10y = -7 - 15k$$

On passe modulo 9 pour obtenir :

$$y \equiv 2 + 3k \text{ [9]}$$

C'est-à-dire qu'il existe $k' \in \mathbb{Z}$ tel que : $y = 2 + 3k + 9k'$. On reporte à nouveau dans l'équation de départ :

$$9x + 10(2 + 3k + 9k') = -7 - 15k \Leftrightarrow x = -3 - 5k - 10k'$$

Finalement, les éventuelles solutions sont :

$$\begin{cases} x = -3 - 5k - 10k' \\ y = 2 + 3k + 9k' \\ z = 1 + 2k \end{cases} \quad \text{où } (k, k') \in \mathbb{Z}^2$$

- **Synthèse.** On injecte dans l'équation pour vérifier :

$$18x + 20y + 15z = 18(-3 - 5k - 10k') + 20(2 + 3k + 9k') + 15(1 + 2k) = 1$$

Nous avons bien trouvé toutes les solutions.

$$\boxed{\mathcal{S} = \{(-3 - 5k - 10k', 2 + 3k + 9k, 1 + 2k),\ (k, k') \in \mathbb{Z}^2\}}$$

4 Soient a et b deux entiers naturels supérieurs ou égaux à 2 avec $\text{pgcd}(a, b) = 1$. Démontrer que $\dfrac{\ln(a)}{\ln(b)}$ est irrationnel.

Corrigé : Par l'absurde, on suppose que $\dfrac{\ln(a)}{\ln(b)} = \dfrac{p}{q}$ avec $(p, q) \in (\mathbb{N}^*)^2$. Cela donne :

$$q \ln(a) = p \ln(b) \Leftrightarrow \ln(a^q) = \ln(b^p) \Leftrightarrow a^q = b^p$$

Ceci est absurde car a et b sont premiers entre eux et supérieurs ou égaux à 2 donc ils ne peuvent se diviser l'un l'autre.

$$\boxed{\frac{\ln(a)}{\ln(b)} \text{ est irrationnel}}$$

4 ★★

1. Soit $n \in \mathbb{N}$ et $(a, b) \in \mathbb{N}^2$. Factoriser $a^{2n+1} + b^{2n+1}$.
2. En déduire que si $2^n + 1$ est premier alors n est une puissance de 2.
3. Pour tout $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$.
4. Démontrer que pour tout $n \in \mathbb{N}$:
$$F_{n+1} = \prod_{k=0}^{n} F_k + 2$$
5. En déduire que si m et n sont deux entiers naturels distincts alors F_m et F_n sont premiers entre eux.

Corrigé :

1. On utilise la formule "$a^n - b^n$" :
$$a^{2n+1} + b^{2n+1} = a^{2n+1} - (-b)^{2n+1} = (a - (-b)) \sum_{k=0}^{2n} a^k (-b)^{2n-k} = (a + b) \sum_{k=0}^{2n} a^k (-b)^{2n-k}$$

2. Par contraposée, si n n'est pas une puissance de 2 alors n possède un diviseur impair supérieur ou égal à 3, on peut écrire $n = pq$ avec $p \geq 3$ et $q \geq 1$. En appliquant la formule de la question précédente, on a :
$$2^n + 1 = (2^q)^p + 1^p = (2^q + 1) \sum_{k=0}^{p-1} (2^q)^k (-1)^{p-1-k}$$
Cette factorisation est non triviale car $1 < 2^q + 1 < (2^q)^p + 1$. On en déduit que $2^n + 1$ n'est pas premier. Ce qui démontre la propriété annoncée par contraposition.

3. On peut démontrer la propriété annoncée par récurrence sur $n \in \mathbb{N}$.

   • **Initialisation.** Si $n = 0$, l'égalité devient $F_1 = F_0 + 2$ ce qui est vrai car $F_0 = 3$ et $F_1 = 5$.

   • **Hérédité.** On suppose la formule vraie au rang $n \in \mathbb{N}$. On a :

   $$F_{n+1} = \prod_{k=0}^{n} F_k + 2 \Leftrightarrow 2^{2^{n+1}} - 1 = \prod_{k=0}^{n} F_k$$

   On multiplie cette inégalité par $F_{n+1} = 2^{2^{n+1}} + 1$ et on reconnait une identité remarquable pour obtenir :

   $$\left(2^{2^{n+1}} + 1\right)\left(2^{2^{n+1}} - 1\right) = 2^{2^{n+2}} - 1 = \prod_{k=0}^{n+1} F_k$$

   C'est-à-dire : $F_{n+2} = \prod_{k=0}^{n+1} F_k + 2$ ce qui est la formule voulue au rang $n+1$. Cela termine la récurrence.

4. Soient m et n deux entiers naturels distincts, on suppose sans perte de généralité que $m > n$, d'après la question précédente :

   $$F_m - \prod_{k=0}^{m} F_k = 2$$

   On remarque que dans le produit le facteur F_n apparait car $n < m$. Soit d un diviseur commun positif de F_n et F_m alors d'après l'égalité précédente, on sait que $d|2$ donc $d = 2$ ou $d = 1$. Les entiers F_m et F_n sont impairs donc ne sont pas divisibles par 2, on vient donc de démontrer que le seul diviseur positif de F_m et F_n vaut 1 : ils sont premiers entre eux.

   $$\boxed{\forall (m,n) \in \mathbb{N}^2,\ m \neq n \Rightarrow F_m \wedge F_n = 1}$$

5 ★★★ Soit $n \geq 2$, démontrer que $n^4 + 4^n$ n'est pas premier.

Corrigé : Si n est pair alors $n^4 + 4^n$ est pair et strictement supérieur à 2, donc n'est pas premier. Il reste à démontrer le résultat pour n impair, notons $n = 2k+1$ avec $k \in \mathbb{N}^*$. On a :

$$n^4 + 4^n = n^4 + 4 \times 4^{2k} = n^4 + 4 \times (2^k)^4$$

Grâce à Sophie Germain, on sait factoriser $a^4 + 4b^4$:

$$a^4 + 4b^4 = a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2)^2 - (2ab)^2 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$$

Ici cela donne :

$$n^4 + 4^n = n^4 + 4 \times (2^k)^4 = (n^2 + 2^{2k+1} + 2^{k+1}n)(n^2 + 2^{2k+1} - 2^{k+1}n)$$

Cette factorisation est non triviale car $a^2 + 2b^2 + 2ab > 1$ et $a^2 + 2b^2 - 2ab > 1$ dès que $a \geq 1$ et $b \geq 1$.

$$\boxed{\forall n \geq 2,\ n^4 + 4^n \text{ n'est pas premier}}$$

6 ★★ (Théorème des Ckicken Nuggets) Dans un célèbre fast-food, il y a des boîtes de 4 ou de 9 chicken nuggets ; les boîtes de 6 étant en rupture de stock ce jour-là. Le but de l'exercice est de décrire les nombres de chicken nuggets qu'il est possible d'atteindre en achetant un mélange de boîtes de 4 ou de 9 chicken nuggets, puis de généraliser le résultat obtenu.

1. (a) Montrer qu'il est impossible d'obtenir exactement 23 chicken nuggets.
   (b) Démontrer que l'on peut obtenir exactement 24, 25, 26 et 27 chicken nuggets.
   (c) En déduire que pour tout entier n supérieur ou égal à 24, on peut obtenir exactement n chicken nuggets.
2. Plus généralement, on considère $(a,b) \in (\mathbb{N}^*)^2$. On s'intéresse à l'ensemble $\Gamma_{a,b} = \{ka + lb,\ (k,l) \in \mathbb{N}^2\}$.
   (a) Démontrer que si a et b ne sont pas premiers entre eux alors il y a une infinité d'entiers naturels qui n'appartiennent pas à $\Gamma_{a,b}$.
   (b) On suppose dans cette question que a et b sont premiers entre eux et on considère un entier naturel $n \geq (a-1)(b-1)$.
      i. Soient $(l,l') \in [\![0, a-1]\!]^2$ tels que $n - lb \equiv n - l'b\ [a]$. Démontrer que $l = l'$.
      ii. En déduire qu'il existe $k \in \mathbb{Z}$ et $l \in [\![0, a-1]\!]$ tels que $n = ka + lb$.
      iii. Justifier que $k \in \mathbb{N}$.
      iv. En déduire qu'il y a un nombre fini d'entiers qui n'appartiennent pas à $\Gamma_{a,b}$.
3. À l'aide de la question 2, expliquer comment se généralise l'exemple de la question 1.

Corrigé :

1. (a) On peut raisonner sur le nombre de boîtes de 4 chicken nuggets qu'il faut acheter pour arriver à 23.
   - Si l'on achète 0 boîte de 4, il est impossible d'atteindre 23 avec uniquement des boîtes de 9.
   - Si l'on achète 1 boîte de 4, il est impossible d'atteindre 19 avec uniquement des boîtes de 9.
   - Si l'on achète 2 boîtes de 4, il est impossible d'atteindre 15 avec uniquement des boîtes de 9.
   - Si l'on achète 3 boîtes de 4, il est impossible d'atteindre 11 avec uniquement des boîtes de 9.
   - Si l'on achète 4 boîtes de 4, il est impossible d'atteindre 7 avec uniquement des boîtes de 9.
   - Si l'on achète 5 boîtes de 4, il est impossible d'atteindre 3 avec uniquement des boîtes de 9.

   On ne peut pas obtenir exactement 23 chicken nuggets

   (b) On a les décompositions suivantes :
   - $24 = 4+4+4+4+4+4$
   - $25 = 4+4+4+4+9$
   - $26 = 4+4+9+9$
   - $27 = 9+9+9$

   Il est possible d'obtenir 24, 25, 26 ou 27 chicken nuggets

   (c) Soit $n \geq 24$, on pose $n' = n - 24$. Effectuons la division euclidienne de n' par 4 :

   $$\exists (q,r) \in \mathbb{N}^2,\ n' = 4q + r \quad \text{avec } 0 \leq r \leq 3$$

   On remarque que le quotient q est bien positif puisque n' est positif. Comme $n = n' + 24$, on a

   $$n = 4q + (24 + r)$$

   D'après la question précédente, pour tout $r \in [\![0,3]\!]$, $24 + r$ peut être atteint avec des boîtes de 4 ou de 9 et $4q$ peut être atteint également en prenant q boîtes de 4.

   Si $n \geq 24$, il est possible d'obtenir n chicken nuggets

2. (a) Soit $(a,b) \in (\mathbb{N}^*)^2$, on suppose que a et b ne sont pas premiers entre eux, c'est-à-dire qu'il existe un entier naturel $d \geq 2$ tel que $d|a$ et $d|b$. Ainsi pour tous k et l des entiers naturels, on a $d|ka + lb$. En résumé, les entiers naturels qui appartiennent à $\Gamma_{a,b}$ sont tous divisibles par d. Les entiers qui ne sont pas divisibles par d n'appartiennent pas à $\Gamma_{a,b}$, il y en a clairement une infinité ; par exemple tous ceux de la forme $dr + 1$ où $r \in \mathbb{N}$.

   Si a et b ne sont pas premiers entre eux alors $\mathbb{N} \setminus \Gamma_{a,b}$ est infini

(b) i. Soient $(l,l') \in [\![0,a-1]\!]^2$. On suppose que $n-lb \equiv n-l'b$, en simplifiant cela donne $b(l'-l) \equiv 0\ [a]$, c'est-à-dire que $a|b(l'-l)$. Or a et b sont premiers entre eux ainsi d'après le théorème de Gauss, $a|l'-l$. D'autre part, on a $(l,l') \in [\![0,a-1]\!]^2$ ce qui implique que $l'-l \in [\![-(a-1),a-1]\!]$. Le seul multiple de a appartenant à cet intervalle est 0, ce qui démontre que $l=l'$.

$$\boxed{l=l'}$$

ii. D'après la question précédente lorsque l décrit $[\![0,a-1]\!]$, l'entier $n-lb$ ne prend que des valeurs différentes modulo a, c'est-à-dire qu'il y a a valeurs différentes prises modulo a. Ainsi, il existe $l \in [\![0,a-1]\!]$ tel que $n-lb \equiv 0\ [a]$. Par définition de la relation de congruence, cela signifie qu'il existe $k \in \mathbb{Z}$ tel que $n-lb=ka$.

$$\boxed{\exists (k,l) \in \mathbb{Z} \times [\![0,a-1]\!],\ n=ka+lb}$$

On peut également utiliser le fait qu'une fonction injective d'un ensemble fini dans lui-même est surjective.

iii. En utilisant la condition de l'énoncé $n \geq (a-1)(b-1)$ et le fait que $l \leq a-1$, on a :

$$ka = n-lb \geq (a-1)(b-1)-(a-1)b = -a+1 \Leftrightarrow (k+1)a \geq 1$$

Comme $a \geq 1$, l'inégalité précédente implique $k \geq 0$.

$$\boxed{\exists (k,l) \in \mathbb{N} \times [\![0,a-1]\!],\ n=ka+lb}$$

iv. Les trois questions précédentes démontrent que pour tout $n \geq (a-1)(b-1)$, on a $n \in \Gamma_{a,b}$ ainsi il n'y a qu'un nombre fini d'entiers qui n'appartient pas à $\Gamma_{a,b}$.

$$\boxed{\text{Si } a \text{ et } b \text{ sont premiers entre eux alors } \mathbb{N} \setminus \Gamma_{a,b} \text{ est fini}}$$

3. Dans l'exemple de la question 1, on a 4 et 9 qui sont premiers entre eux. D'après la question 2. cela permet d'affirmer que pour tout entier supérieur à $(4-1)(9-1)=24$ s'écrit comme combinaison à coefficients positifs de 4 et 9, ce qui nous avons effectivement vérifié dans la question 1. La question 2 démontre que l'on peut remplacer 4 et 9 par deux entiers premiers entre eux, a et b, pour obtenir que tout nombre entier naturel à partir d'un certain rang est combinaison à coefficients positifs de a et b. De plus, le rang $(a-1)(b-1)$ convient.

Le problème étudié se généralise à plus de deux entiers. Si l'on se donne p entiers : $1<a_1<a_2<...<a_p$, un entier N quelconque peut-il s'exprimer comme une combinaison : $N=k_1a_{p_1}+k_2a_{p_2}...+k_pa_p$ où les coefficients k_1,...,k_p sont des entiers positifs ? On sait démontrer que si les $(a_i)_{1\leq i\leq p}$ sont premiers entre eux, il n'y a qu'un nombre fini d'entiers N qui ne peuvent pas s'écrire ainsi et le plus grand d'entre eux est noté $g(a_1,...,a_p)$ (nombre de Frobenius de la famille $(a_i)_{1\leq i\leq p}$). On a vu que $g(4,9)=23$ et plus généralement $g(a,b)=(a-1)(b-1)-1$. On ne connait pas de formule explicite pour $g(a_1,...,a_p)$ si $p \geq 3$.

Ce problème est également lié au suivant : quel système de monnaie faut-il adopter afin d'obtenir une somme inférieure à 1 euro en un minimum de pièces ? Par exemple, si l'on s'autorise 6 pièces, il est optimal de choisir des pièces de 1, 2, 5, 11, 25 et 62 centimes d'euros. Il faudra alors en moyenne 3,13 pièces pour obtenir une somme inférieure à 1 euro.

7 ★★ Trouver tous les $(x,y) \in \mathbb{N}^2$ tels que :

$$(x \vee y)^2 - 5(x \wedge y)^2 = 2000$$

où $x \vee y = \text{ppcm}(x,y)$ et $x \wedge y = \text{pgcd}(x,y)$.

Corrigé : • **Analyse.** On se donne $(x,y) \in \mathbb{N}^2$ vérifiant l'équation. Pour simplifier, on note $d=\text{pgcd}(x,y)$ et $m=\text{ppcm}(x,y)$. On a $d|m$ donc $d^2|m^2-5d^2=2000$. On décompose 2000 en facteurs premiers :

$$2000 = 2^4 \times 5^3$$

ce qui nous permet de trouver les entiers d tels que $d^2|2000$, on a $d \in \{1,2,4,5,10,20\}$. De plus $m=\sqrt{2000+5d^2}$ doit être un entier. On peut vérifier (éventuellement à l'aide d'une calculatrice) que seul $d=10$ convient et dans ce cas $m=50$. Ce qui nous ramène à résoudre le système :

$$\begin{cases} x \wedge y = 10 \\ x \vee y = 50 \end{cases}$$

On peut écrire $x = 10x'$ et $y = 10y'$ avec $x' \wedge y' = 1$. On sait que $xy = md = 500$ donc $x'y' = 5$. On en déduit que $(x', y') \in \{(1,5),(5,1)\}$ et

$$(x, y) \in \{(10, 50), (50, 10)\}$$

• **Synthèse.** On vérifie par un calcul direct que ces deux couples conviennent.

$$\boxed{\mathcal{S} = \{(10, 50), (50, 10)\}}$$

9 ★ Soient $(a, b) \in \mathbb{Z}^2$ et $(n, p) \in \mathbb{N}^2$. On suppose que $p|n$, démontrer que $(a^p - b^p)|(a^n - b^n)$.

Corrigé : Par hypothèse, il existe $k \in \mathbb{N}$ tel que $pk = n$. On a :

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

Ce qui démontre que $(a^p - b^p)|(a^n - b^n)$.

10 Trouver tous les $(x, y) \in \mathbb{Z}^2$ tels que $\dfrac{1}{2x} + \dfrac{1}{y} = \dfrac{1}{10}$.

Corrigé : Pour $(x, y) \in \mathbb{Z}^2$ non nuls, on a : $\dfrac{1}{2x} + \dfrac{1}{y} = \dfrac{1}{10}$

" $\Leftrightarrow$ $\dfrac{5y + 10x}{10xy} = \dfrac{xy}{10xy}$
" $\Leftrightarrow$ $10x + 5y = xy$
" $\Leftrightarrow$ $(x - 5)(y - 10) = 50$
" $\Leftrightarrow$ $(x - 5, y - 10) \in \{(1,50),(2,25),(5,10),(10,5),(25,2),(50,1),(-1,-50),(-2,-25),(-5,-10),(-10,-5),(-25,-2),(-50,-1)\}$
" $\Leftrightarrow$ $(x, y) \in \{(6,60),(7,35),(10,20),(15,15),(30,12),(55,11),(4,-40),(3,-15),\cancel{(0,0)},(-5,5),(-20,8),(-45,9)\}$

11 ★ Soient $(a, b) \in \mathbb{Z}^2$ premiers entre eux. Démontrer que $a + b$ et ab sont premiers entre eux.

Corrigé : Par l'absurde si $a + b$ et ab ne sont pas premiers entre eux, ils admettent un diviseur $d \geq 2$, ce diviseur a lui même un diviseur premier p. On a $p|d$ et $d|ab$ donc $p|ab$, étant donné que p est premier, on en déduit que $p|a$ ou $p|b$. On suppose que $p|a$, l'autre cas étant identique.

On a aussi $p|a + b$ donc $p|a + b - a = b$, ainsi p est un diviseur premier de a et b : c'est absurde.

On peut aussi résoudre cet exercice en considérant des relations de Bézout.