

Feuille 1 : Arithmétique dans \mathbb{Z} **Exercice 1.**

1. Donner la liste des entiers positifs qui divisent 100.
2. Combien le nombre 6000000 a-t-il de diviseurs positifs ?
3. Combien $13!$ admet-il de diviseurs ?

Exercice 2. Combien d'entiers strictement compris entre 101 et 1001 sont divisibles par 7 ?

Exercice 3. La différence de deux nombres entiers est 538. Si l'on divise l'un par l'autre, le quotient est 13 et le reste 22. Quels sont ces nombres ?

Exercice 4. Quels sont les restes possibles de la division euclidienne d'un entier impair par 4 ? En déduire que le reste du carré d'un entier impair dans la division euclidienne par 8 est 1.

Exercice 5. Les nombres a, b, c, d étant des éléments non nuls de \mathbb{Z} , dire si les propriétés suivantes sont vraies ou fausses, en justifiant la réponse.

1. Si a divise b et b divise c , alors a divise c .
2. Si a divise b et c , alors a divise $2b + 3c$.
3. Si a divise b et c , alors $c^2 - 2b$ est multiple de a .
4. S'il existe u et v entiers tels que $au + bv = 4$ alors $\text{pgcd}(a, b) = 4$.
5. Si a est premier avec b , alors a est premier avec b^3 .
6. Si a divise $b + c$ et $b - c$, alors a divise b et a divise c .
7. Si $7a - 9b = 1$ alors a et b sont premiers entre eux.
8. Si a divise b et b divise c et c divise a , alors $|a| = |b|$.
9. Si 19 divise ab , alors 19 divise a ou 19 divise b .
10. Si a est multiple de b et si c est multiple de d , alors $a + c$ est multiple de $b + d$.
11. « a et b premiers entre eux » équivaut à « $\text{ppcm}(a, b) = |ab|$ ».
12. Si a divise c et b divise d , alors ab divise cd .
13. Si 9 divise ab et si 9 ne divise pas a , alors 9 divise b .
14. Si a divise b ou a divise c , alors a divise bc .
15. « a divise b » équivaut à « $\text{ppcm}(a, b) = |b|$ ».
16. Si a divise b , alors a n'est pas premier avec b .
17. Si a n'est pas premier avec b , alors a divise b ou b divise a .
18. Si 4 ne divise pas bc , alors b ou c est impair.
19. Si a divise b et b ne divise pas c , alors a ne divise pas c .

20. Si 5 divise b^2 , alors 25 divise b^2 .
21. Si 12 divise b^2 , alors 4 divise b .
22. Si 12 divise b^2 , alors 36 divise b^2 .
23. Si 91 divise ab , alors 91 divise a ou 91 divise b .

Exercice 6.

1. Montrer que le produit de trois nombres consécutifs est divisible par 6.
2. Montrer que le produit de quatre nombres consécutifs est divisible par 24.

Exercice 7. Pour chaque entier $n \in \{8, 16, 6, 12, 30, 90, 98, 72, 8100, 900\}$ trouver le plus petit entier positif m tel que n divise m^2 .

Exercice 8. Ecrire le nombre 2017 en base 7.

Exercice 9. Soit n l'entier naturel dont l'écriture en base 9 est 512121. Ecrire n en base 10.

Exercice 10. Ecrire en base 7 le nombre qui s'écrit 713 en base 8.

Exercice 11.

1. Décomposer $10!$ en produit de facteurs premiers.
2. Trouver la plus grande puissance de 2 qui divise $100!$.
3. Trouver le nombre de zéros qui figurent à la fin de l'écriture décimale de $100!$.

Exercice 12. Soit $n \in \mathbb{N}^*$. On considère M_n l'entier dont l'écriture en base 2 est composée de n un. Par exemple, $M_3 = 111$. Donner l'écriture en base deux de M_n^2 .

Exercice 13. Trouver le pgcd et le ppcm de $a = 2^3 \times 3^5 \times 7^2$ et $b = 2 \times 5^2 \times 7^3$.

Exercice 14. Soit n un entier tel que $10 \leq n \leq 100$. Montrer que n est un nombre premier si et seulement si $\text{pgcd}(n, 210) = 1$.

Exercice 15. Soit a, b, c des entiers non nuls.

1. Montrer que $\text{pgcd}(ca, cb) = |c| \text{pgcd}(a, b)$.
2. Montrer que $\text{pgcd}(a^2, b^2) = (\text{pgcd}(a, b))^2$.
3. Montrer que si $\text{pgcd}(a, b) = 1$ et si c divise a , alors $\text{pgcd}(c, b) = 1$.
4. Montrer que $\text{pgcd}(a, bc) = 1$ si et seulement si $\text{pgcd}(a, b) = \text{pgcd}(a, c) = 1$.
5. Montrer que si $\text{pgcd}(a, b) = 1$ alors $\text{pgcd}(a + b, a - b) = 1$ ou 2 et $\text{pgcd}(a + b, ab) = 1$

Exercice 16. Soit n un entier positif. Que vaut $\text{pgcd}(n, n + 1)$ et $\text{ppcm}(n, n + 1)$?

Exercice 17.

1. Calculer le pgcd de 637 et 595.
2. Trouver les entiers x et y tels que $637x + 595y = 91$.
3. Trouver les entiers x et y tels que $637x + 595y = 143$.

Exercice 18. Résoudre les équations suivantes en nombres entiers :

1. $283x + 1722y = 31$.
2. $365x + 72y = 18$.
3. $101x + 150y = 15$
4. $282x + 678y = 66$.

Exercice 19. Résoudre le système dans \mathbb{N}^2 donné par $\text{pgcd}(a, b) = 12$ et $\text{ppcm}(a, b) = 360$.

Exercice 20. Déterminer les couples d'entiers naturels de pgcd 9 et de somme 360.
De même avec pgcd 18 et produit 1620.

Exercice 21.

1. Déterminer une solution particulière dans \mathbb{Z} de l'équation $7x + 16y = 1$.
2. Donner toutes les solutions dans \mathbb{Z} de l'équation $7x + 16y = 1$.
3. Alice est au bord d'un lac, et possède deux récipients, un de 7 litres et l'autre de 16 litres.
 - (a) En utilisant ce qui précède, montrer qu'Alice peut en remplissant ou en vidant le contenu des deux récipients un certain nombre de fois et dans un ordre approprié, obtenir exactement 1 litre d'eau dans l'un des deux récipients.
 - (b) Donner une solution du problème qui utilise un nombre minimal de remplissage du récipient de 16 litres.
4. Alice possède maintenant un récipient de 14 litres et un autre de 21 litres. Peut elle obtenir exactement 1 litre d'eau ?

Exercice 22. Soit n un entier ≥ 1 . Montrer qu'il existe n nombres entiers consécutifs qui ne sont pas premiers.

Indication : considérer $(n+1)! + 2, (n+1)! + 3, \dots$

Exercice 23. Soit p un nombre premier tel que $11p + 1$ est le carré d'un entier. Déterminer p .**Exercice 24.** Soit a et b deux entiers premiers entre eux (i.e. $\text{pgcd}(a, b) = 1$). On suppose que $ab = c^2$. Montrer que a et b sont eux-mêmes des carrés au signe près.**Exercice 25.** Soit b un entier positif non nul. Montrer que l'entier qui s'écrit 10101 en base b n'est pas un nombre premier.**Exercice 26.** Vérifier que si un entier positif n est à la fois un carré et un cube, alors il existe $k \in \mathbb{N}$ tel que $n = 7k$ ou $n = 7k + 1$.

Exercice 27. Soient $a, b \in \mathbb{N}^*$ tels que $a^9 = b^{25}$.

1. Trouver u et $v \in \mathbb{Z}$ tels que $25u + 9v = 1$.
2. Soit $c = a^u b^v$, montrer que $c^{25} = a$ et $c^9 = b$.
3. Soit $x \in \mathbb{Q}$, supposons qu'il existe un entier $k \in \mathbb{N}^*$ tel que $x^k \in \mathbb{Z}$. Montrer que $x \in \mathbb{Z}$.
4. En déduire que $c \in \mathbb{N}^*$.
5. Plus généralement, soient m, n premiers entre eux tels que $a^m = b^n$. Montrer qu'il existe $c \in \mathbb{N}^*$ tel que $c^n = a$ et $c^m = b$.

Feuille 1 : éléments de correction

Ex 1 q1) Il s'agit de 1, 2, 4, 5, 10, 20, 25, 50, 100 car $100 = 2^2 \cdot 5^2$ donc si $d \mid 100$ alors $d = 2^i 5^j$ avec $0 \leq i \leq 2$ et $0 \leq j \leq 2$.
 et $1 = 2^0 \cdot 5^0$, $2 = 2^1 \cdot 5^0$, $4 = 2^2 \cdot 5^0$, $5 = 2^0 \cdot 5^1$, $10 = 2^1 \cdot 5^1$, $20 = 2^2 \cdot 5^1$, $25 = 2^0 \cdot 5^2$, $50 = 2^1 \cdot 5^2$, $100 = 2^2 \cdot 5^2$ sont les 9 diviseurs possibles.

q2) On a $6\ 000\ 000 = 6 \cdot 10^6 = 3 \cdot 2^7 \cdot 5^6 = 2^7 \cdot 3 \cdot 5^6$ donc si $d \mid 6\ 000\ 000$ alors $d = 2^\alpha 3^\beta 5^\gamma$ avec $0 \leq \alpha \leq 7 \rightarrow 8$ possibilités $0 \leq \beta \leq 1 \rightarrow 2$ possibilités $0 \leq \gamma \leq 6 \rightarrow 7$ possibilités.

Par conséquent 6 000 000 admet $8 \cdot 2 \cdot 7 = 112$ diviseurs possibles.

q3) La décomposition en facteurs premiers de $13! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ est $13! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ donc d'après le raisonnement des deux premières questions $13!$ admet $11 \cdot 6 \cdot 3 \cdot 2 \cdot 2 \cdot 2 = 1584$ diviseurs possibles.
 Si on veut compter aussi les diviseurs négatifs, il suffit d'en prendre deux fois plus, c'est 3168 diviseurs possibles ou négatifs.

Ex 2 On a $105 = 7 \cdot 15$ et $994 = 7 \cdot 142$ et si $101 < n < 1001$ et $n = 7k$ alors $7 \cdot 15 \leq n = 7k \leq 7 \cdot 142$ avec $15 \leq k \leq 142$.
 jusqu'à k peut prendre $142 - 14 = 128$ valeurs, il y a 128 entiers divisibles par 7, strictement compris entre 101 et 1001.
 On connaît un diviseur aussi $14 \left[\frac{101}{7} \right] < k \leq \left[\frac{1001}{7} \right] = 143$.

Ex 3 Si on note a et b les deux nombres il s'agit de résoudre

$$\begin{cases} a = 538 + b \\ a = 13b + 22 \end{cases} \quad \text{on} \quad \begin{cases} a = 538 + b \\ b = 13a + 22 \end{cases}. \quad \text{Le premier système devient}$$

$12b = 516$ donc $\begin{cases} b = 43 \\ a = 581 \end{cases}$. Le second devient $-12a = 560$ qui n'a pas de solutions en nombres entiers car 3 ne divise pas 560.

Ex 4 On a $2k+1 = 4q+r$ avec $0 \leq r \leq 4$. Comme $4q+r$ est impair, on exclut les cas $r=0$ ou $r=2$, ce qui nous laisse les possibilités $r=1$ ou $r=3$, qui peuvent arrêter toutes les deux, par exemple pour $2k+1 = 5 = 4 \cdot 1 + 1$ ou pour $2k+1 = 7 = 4 \cdot 1 + 3$.

$$\text{On a donc } (2k+1)^2 = (4q+1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1$$

$$\text{ou bien } (2k+1)^2 = (4q+3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1$$

ce qui signifie exactement que le reste de la division euclidienne de $(2k+1)^2$ par 8 est toujours 1.

On aurait pu se convaincre de cela aussi en élevant directement $(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$ et en remarquant que $k(k+1) \in 2\mathbb{Z}$ est un autre gain en tant que produit de deux entiers consécutifs.

$$\boxed{\text{Ex5}} \quad \text{q1)} \quad \text{On a } \boxed{b = ka} \text{ et } \boxed{c = lb} \text{ donc } c = lka \text{ donc } a \mid c.$$

$$\text{q2)} \quad \text{On a } \boxed{b = ka} \text{ et } \boxed{c = la} \text{ donc } 2b + 3c = 2ka + 3la = a(2k + 3l) \\ \text{c'est à dire } a \mid c.$$

$$\text{q3)} \quad \text{On a } \boxed{b = ka} \text{ et } \boxed{c = la} \text{ donc } c^2 - 2b = l^2a^2 - 2ka = a(l^2a - 2k) \\ \text{d'où } a \mid c.$$

$$\text{q4)} \quad \text{Cette affirmation est fausse car par exemple si } a \text{ et } b \text{ sont premiers entre eux, d'après le théorème de Bezout, } \exists \alpha \text{ et } \beta \in \mathbb{Z} \text{ tels que } 1 = \alpha a + \beta b. \text{ En multipliant par 4 cette égalité on a } 4 = 4\alpha a + 4\beta b \text{ avec } u = 4\alpha \text{ et } v = 4\beta \text{ entiers, sans que pgcd}(a, b) \text{ soit égal à 4. Exemple numérique: } a = b = 1, \alpha = 2, \beta = -1,$$

$$u = 8, v = -4. \text{ On a bien } 8 \cdot 1 - 4 \cdot 1 = 4 \text{ et } \text{pgcd}(1, 1) = 1 \neq 4.$$

$$\text{q5)} \quad \text{Si } \text{pgcd}(a, b^3) \neq 1, \text{ il existe un premier } p \text{ tel que } p \mid a \text{ et } p \nmid b^3.$$

Alors p est un facteur premier de b^3 , qui a les mêmes facteurs premiers que b . Donc $p \mid b$, par conséquent $p \nmid \text{pgcd}(a, b) = 1$ ce qui contredit notre hypothèse de départ. En conclusion $\text{pgcd}(a, b^3) = 1$ et l'affirmation est vraie.

$$\text{q6)} \quad \text{Cette affirmation est fausse car si } b \text{ et } c \text{ sont impairs, on a bien pour } a = 2 \text{ que } 2 \mid b+c \text{ et } 2 \mid b-c \text{ sans que } 2 \mid b \text{ ou } 2 \mid c.$$

Exemple numérique: $a = 2, b = c = 1$.

$$\text{q7)} \quad \text{Si } p \mid a \text{ et } p \nmid b \text{ alors } p \mid 7a - 9b = 1 \text{ donc } p = \pm 1 \text{ ce qui signifie bien que } \text{pgcd}(a, b) = 1, \text{ donc que } a \text{ et } b \text{ sont premiers entre eux.}$$

ex5. q8) On doit avoir $b = ka$, $c = lb$ et $a = sc = slb = slka$ avec $s, l, k \in \mathbb{Z}$. Par conséquent $a(1 - slk) = 0$. Si $a \neq 0$ alors $b = c = 0$ et $|a| = |b|$. Si $a \neq 0$ alors $1 = slk$ donc $k = \pm 1$ c'est encore $|a| = |b|$.

q9) lorsque 19 est premier, et $19 \mid ab$, c'est que 19 apparaît comme facteur premier de $a \cdot b$. Par conséquent 19 est facteur premier de a ou de b donc $19 \mid a$ ou $19 \mid b$.

q10) On peut écrire $a = kb$ et $c = ld$ ce qui donne $a + c = kb + ld$ sans pouvoir conclure à une égalité $a + c = s(b + d)$. En effet cette affirmation est fausse. Exemple numérique : $a = b = d = 1$, $c = 2$ et $a + c = 3$ n'est pas multiple de $b + d = 2$.

q11) On a $\text{pgcd}(a, b) \text{ppcm}(a, b) = |ab|$ car si $a = \prod p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ et $b = \prod q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}$ sont les décompositions en produits de facteurs premiers (distincts) de a et b on ait que $\text{pgcd}(a, b) = \prod_{i=1}^s p_i^{\min(\alpha_i, \beta_i)}$

$$\text{ppcm}(a, b) = \prod_{i=1}^t p_i^{\max(\alpha_i, \beta_i)}$$

On $\alpha_i + \beta_i = \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i)$ d'où l'égalité annoncée.

Par conséquent $\text{ppcm}(a, b) = |ab|$ si $\text{pgcd}(a, b) = 1$ si a et b sont premiers entre eux.

q12) En effet si $c = ka$ et $d = lb$, on a $cd = kka \cdot lkb$ donc $ab \mid cd$.

q13) Cette affirmation est fausse car 9 n'est pas premier donc on peut avoir $3 \mid a$ et $3 \mid b$ donc $9 \mid ab$ sans que 9 divise b .

Exemple numérique $a = b = 3$.

q14) Si $b = ka$ on a $bc = kac$ donc $a \mid bc$.

Si $c = la$ on a $bc = lab$ donc $a \mid bc$.

q15) Si a divise b alors $|b|$ est un multiple de a et de b .

Si c est un multiple de a et de b alors c est un multiple de $|b|$ donc $\text{ppcm}(a, b) \mid |b|$ (qui est par définition le plus petit commun multiple positif de a et de b)

Si $\text{ppcm}(a, b) \mid |b|$ c'est que $a \mid |b|$ donc que $a \mid b$.

Donc l'affirmation est vraie.

q16) Si $a \neq 1$ alors a divise le pour tout $b \in \mathbb{Z}$

Tout en étant premier à b . Donc l'affirmation est fausse. En fait elle est équivalente à $\text{pgcd}(a, b) = 1$ et pour $(ab=1)$, a est premier à b .

q17) cette affirmation est fausse car on peut avoir par exemple $a=4, b=6$, $\text{pgcd}(a, b)=2 \neq 1$ et $4+6$ est $6+4$.

q18) En effet si b et c sont pairs, alors $2|b$ et $2|c$ donc $b=2b'$, $c=2c'$, d'où $bc=4b'c'$ c'est $4|bc$.

Par conséquent si $4|bc$ on doit avoir b ou c impair.

q19) Cette affirmation est fausse car par exemple si $a=2, b=4$ et $c=2$ on a bien $a|b$, $b|c$ et $a|c$.

q20) Si $5|b^2$ alors $5|b$ car 5 est premier (et un facteur premier de b^2 est un facteur premier de b). Alors $b=5b'$ donc $b^2=25b'^2$ d'où $25|b^2$.

q21) Si $12=2^2 \cdot 3$ divise b^2 alors $2|b^2$ et $3|b^2$ donc $6|b^2$ or $4|b^2$

q18) mais on ne peut pas conclure que $4|b$. En effet l'affirmation est fausse en prenant par exemple $b=6$.

q22) D'après q21) on a $2|b^2$ et $3|b^2$ donc $2|b$ et $3|b$.

Puisque 2 et 3 sont premiers entre eux on a que $6|b$ (2 et 3 sont facteurs premiers de b). Donc $b=6b'$, d'où $b^2=36b'^2$ et $36|b^2$.

q23) On a $g_1=7 \cdot 13$ donc g_1 n'est pas premier. Pour $a=7, b=13$ on a bien $g_1|ab$ sans que g_1 divise a ou g_1 divise b . Cette affirmation est donc fausse.

Ex 6 q1) Le produit de deux nombres consécutifs est divisible par 2 car l'un d'eux est forcément pair. Le produit P de trois nombres consécutifs est divisible par 3 car l'un des trois nombres est forcément un multiple de 3. Comme $2|P$ et $3|P$ et que $\text{pgcd}(2, 3) = 1$ on a $6|P$. On peut dire aussi que 2 et 3 sont facteurs premiers de P .

q2) Si Q est le produit de quatre nombres consécutifs on a $3|Q$ d'après la q1). Parmi les quatre nombres il y en a un qui est divisible par 4 et un autre qui est divisible par 2 (différent de celui qui est divisible par 4). Le produit de ces deux nombres est divisible par 8 donc $8|Q$. Comme $\text{pgcd}(3, 8) = 1$ on a $3 \cdot 8 = 24$ qui divise Q .

ex7 Pour $n=8=2^3$ on a $2^3 \mid m^2$ et comme la décomposition de m^2 en facteurs premiers comporte que des puissances paires, on doit avoir $2^4 \mid m^2$. Le plus petit $m > 0$ tel que $16 \mid m^2$ est donc $m=4$.

Pour $n=16$ on a de nouveau $m=4$ car $n=4^2$.

Pour $n=6$ on a $6 \mid m^2$ donc $36 \mid m^2$ d'où $m=6$.

Pour $n=12$ on a $12 \mid m^2$ donc $36 \mid m^2$ d'où $m=6$.

Pour $n=30$ on a $2 \cdot 3 \cdot 5 \mid m^2$ donc $900 \mid m^2$ d'où $m=30$.

Pour $n=90$ on a $2 \cdot 3^2 \cdot 5 \mid m^2$ donc $900 \mid m^2$ d'où $m=30$.

Pour $n=98$ on a $2 \cdot 7^2 \mid m^2$ donc $196 \mid m^2$ d'où $m=14$

Pour $n=72$ on a $2^3 \cdot 3^2 \mid m^2$ donc $144 \mid m^2$ d'où $m=12$.

Pour $n=8100$ on a $90^2 \mid m^2$ donc $m=90$.

Pour $n=900$ on a $30^2 \mid m^2$ donc $m=30$.

ex8

On effectue des divisions successives par 7 :

$$\begin{array}{r} 2017 \\ -14 \quad | \quad 7 \\ \hline 61 \\ -56 \quad | \quad 28 \\ \hline 5 \\ -56 \quad | \quad 1 \\ \hline 1 \end{array}$$

$$\begin{aligned} \text{Donc } 2017 &= 7 \cdot 288 + 1 = \\ &= 7 \cdot (7 \cdot 41 + 1) + 1 = \\ &= 7(7 \cdot (7 \cdot 5 + 6) + 1) + 1 \\ &= 7^3 \cdot 5 + 7^2 \cdot 6 + 7 \cdot 1 + 1 \end{aligned}$$

Cela signifie que $2017_{10} = 5611_7$. On voit que clairement à reprendre dans l'ordre inverse le quotient final et les restes obtenus :

ex9

$$\begin{aligned} n = 512121_9 &= 5 \cdot 9^5 + 1 \cdot 9^4 + 2 \cdot 9^3 + 1 \cdot 9^2 + 2 \cdot 9 + 1 = \\ &= 5 \cdot 59049 + 1 \cdot 6561 + 2 \cdot 729 + 1 \cdot 81 + 2 \cdot 9 + 1 = \\ &= 295245 + 6561 + 4758 + 81 + 18 + 1 = \\ &= 303364_{10} \end{aligned}$$

ex10

$$713_8 = 7 \cdot 8^2 + 1 \cdot 8 + 3 = 7 \cdot 64 + 11 = 459_{10} = 1224_7$$

$$\begin{array}{r} 459 \\ -42 \quad | \quad 65 \\ \hline 39 \\ -35 \quad | \quad 2 \\ \hline 4 \\ -2 \end{array}$$

$$\begin{aligned} \text{Car } 459 &= 7 \cdot 65 + 4 = 7 \cdot (7 \cdot 9 + 2) + 4 = \\ &= 7^2 \cdot 9 + 7 \cdot 2 + 4 \end{aligned}$$

ex. 11

$$91) \quad 10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 =$$

$$\begin{aligned} &= \underbrace{2 \cdot 3 \cdot 2^2}_{\text{pair}} \cdot \underbrace{5 \cdot (2 \cdot 3)}_{\text{pair}} \cdot \underbrace{7 \cdot 2^3}_{\text{pair}} \cdot \underbrace{3^2}_{\text{pair}} \cdot \underbrace{(2 \cdot 5)}_{\text{pair}} \\ &= \underbrace{2^8}_{\text{pair}} \cdot \underbrace{3^4}_{\text{pair}} \cdot \underbrace{5^2}_{\text{pair}} \cdot 7 \end{aligned}$$

92)

Dans le produit $1 \cdot 2 \cdot 3 \cdot 4 \cdots \cdot 100 = 100!$ il y a d'abord une contribution de 1 pour chaque nombre pair dans $\nu_2(100!) =$ la plus grande puissance de 2 qui divise $100!$

(On note $\nu_p(n)$ la plus grande puissance de p qui divise n)

Donc, comme il y a $\frac{100}{2} = 50$ nombres pairs de 1 à 100 on a $\therefore \nu_2(100!) = 50 + \nu_2(50!)$

En effet, en divisant par 2 chacun de ces nombres pairs pour enlever cette contribution on doit s'occuper maintenant de

$$\nu_2(50!) = \nu_2\left(\frac{2}{2} \cdot \frac{4}{2} \cdot \frac{6}{2} \cdots \cdot \frac{100}{2}\right) = \nu_2(1 \cdot 2 \cdot 3 \cdots \cdot 50)$$

On répète le procédé ci-dessus : il y a $\frac{50}{2} = 25$ nombres pairs de 1 à 50 qui apporte chacun une contribution de 1 dans $\nu_2(50!)$, qui sera donc $\nu_2(50!) = 25 + \nu_2(25!)$ car

$$\frac{2}{2} \cdot \frac{4}{2} \cdot \frac{6}{2} \cdots \cdot \frac{50}{2} = 1 \cdot 2 \cdots \cdot 25 = 25!$$

$$\text{On continue de la même manière } \nu_2(100!) = \left[\frac{100}{2}\right] + \left[\frac{50}{2}\right] + \left[\frac{25}{2}\right] + \nu_2(25)$$

$$\text{car } \nu_2(25!) = \nu_2(24!) = 12 + \nu_2\left(\frac{2}{2} \cdot \frac{4}{2} \cdots \cdot \frac{24}{2}\right) \text{ et ainsi de suite}$$

$$\nu_2(12!) = \left[\frac{12}{2}\right] + \nu_2(6!) = \left[\frac{12}{2}\right] + \left[\frac{6}{2}\right] + \nu_2(3!) = 6 + 3 + 1$$

$$\text{Finalement } \nu_2(100!) = \left[\frac{100}{2}\right] + \left[\frac{50}{2}\right] + \left[\frac{25}{2}\right] + \left[\frac{12}{2}\right] + \left[\frac{6}{2}\right] + \left[\frac{3}{2}\right] = 97$$

et on comprend que cette formule se généralise à

$$\nu_2(n!) = \left[\frac{n}{2}\right] + \left\{ \left[\frac{\frac{n}{2}}{2}\right] \right\} + \left[\left[\frac{\left[\frac{n}{2} \right]}{2} \right] \right] + \cdots$$

Pour simplifier la formule montrons que $\left[\frac{\left[\frac{n}{r} \right]}{r} \right] = \left\{ \frac{n}{r^2} \right\}$

Écrivons pour cela la division euclidienne de n par p :

$$n = q_1 \cdot p + r_1 \quad \text{avec } 0 \leq r_1 \leq p-1 \quad \text{et ensuite la}$$

division euclidienne de q_1 par p :

$$q_1 = q_2 \cdot p + r_2 \quad \text{avec } 0 \leq r_2 \leq p-1$$

$$\text{Alors } n = q_1 \cdot p + r_1 = p(pq_2 + r_2) + r_1 = p^2q_2 + pr_2 + r_1$$

$$\text{avec } 0 \leq pr_2 \leq p(p-1)$$

$$0 \leq r_1 \leq p-1$$

$$\overbrace{0 \leq pr_2 + r_1 \leq (p+1)(p-1)} = p^2 - 1$$

Donc $n = p^2q_2 + (pr_2 + r_1)$ est la division euclidienne de n par p^2 . On $\left[\frac{n}{p}\right] = q_1$, $\left[\frac{\frac{n}{p}}{p}\right] = \left[\frac{q_1}{p}\right] = q_2$

$$\text{et } \left[\frac{n}{p^2}\right] = q_2 \text{ d'où l'égalité.}$$

La formule recherchée est donc

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$

qui se généralise encore à

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$

$$\text{Cas particulier : } n=10, p=2 \text{ on a bien } \nu_2(10!) = \left[\frac{10}{2}\right] + \left[\frac{10}{4}\right] + \left[\frac{10}{8}\right] = 8$$

comme à la question 1

$$\text{De même } n=10, p=3 \text{ on a } \nu_3(10!) = \left[\frac{10}{3}\right] + \left[\frac{10}{9}\right] = 3+1=4$$

$$n=10, p=5 \quad , \quad \nu_5(10!) = \left[\frac{10}{5}\right] = 2$$

$$n=10, p=7 \quad , \quad \nu_7(10!) = \left[\frac{10}{7}\right] = 1$$

q3) Le nombre de zéros cherché est la puissance maximale de 10

dans la décomposition de $100!$, obtenue comme $\min(\nu_2(100!), \nu_5(100!))$

car $10=2\cdot 5$ et $\nu_{10}(100!)$ tient compte de la puissance maximale

du "couple" 2.5 dans la décomposition en facteurs premiers de 100!.

$$\text{Or } \varphi_2(100!) = 97 \quad \text{et } \varphi_5(100!) = \left[\frac{100}{5} \right] + \left[\frac{100}{25} \right] = 20 + 4 = 24$$

Donc il y a 24 zeros à la fin de l'écriture décimale de 100! (on peut s'imaginer mieux ainsi l'ordre de grandeur de ce nombre, immense!).

(ex 12)

$$\text{On a } M_n = 2^{n-1} + \dots + 2^2 + 2 + 1 = \frac{2^n - 1}{2 - 1} = 2^n - 1$$

$$\begin{aligned} \text{Par conséquent } M_n^2 &= 2^{2n} - 2^{n+1} + 1 = 2^{2n-1} + 2^{2n-2} - 2^{n+1} + 1 = \\ &= 2^{2n-1} + 2^{2n-2} + 2^{2n-2} - 2^{n+1} + 1 = 2^{2n-1} + 2^{2n-2} + 2^{n+1} + 2^{n+1} - 2^{n+1} + 1 \\ &= 2^{2n-1} + 2^{2n-2} + \dots + 2^{n+1} + 1 = \underbrace{2^{2n-1}}_{2m} + \underbrace{2^{2n-2}}_{m+1} + \dots + \underbrace{2^{n+1}}_{1} - \underbrace{2^{n+1}}_{1} + 1 \\ &= 2M_{2n} - M_{n+1} + M_1 \end{aligned}$$

(ex 13)

$$\text{Si } a = 2^3 \times 3^5 \times 7^2 \text{ et } b = 2 \times 5^2 \times 7^3 \text{ on a}$$

$$\text{pgcd}(a, b) = 2 \times 7^2 \text{ et ppcm}(a, b) = 2^3 \times 3^5 \times 5^2 \times 7^3.$$

(ex 14)

On a $210 = 2 \times 3 \times 5 \times 7$ et comme $\text{pgcd}(n, 210) = 1$ on sait que la décomposition en facteurs premiers de n est

$$n = \prod_{i=1}^{\alpha_1} p_1^{\alpha_1} \cdot \prod_{i=2}^{\alpha_2} p_2^{\alpha_2} \cdots \cdot \prod_{i=21}^{\alpha_{21}} p_{21}^{\alpha_{21}} \text{ avec } \alpha_i \geq 0. \text{ Or } n^2 \geq 100$$

donc parmi $(\alpha_1, \dots, \alpha_{21})$ il n'y a qu'un seul α_i non nul, et α_i est au plus égal à 1. En effet, la présence d'un $\alpha_i \geq 2$ entraîne $n \geq n^2 \geq 100$, et la présence de $\alpha_i = \alpha_j = 1$ entraîne $n \geq 11 \times 13 > 11^2 > 100$. Par conséquent n est premier compris entre 10 et 100 (à savoir $n \in \{11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$).

(ex 15)

9) Cette question a été posée en cours, avec une preuve

qui utilisait l'algorithme d'Euclide. On peut en donner une qui utilise la décomposition de a, b, c en facteurs premiers. Tenez-vous à ce que $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, $b = p_1^{\beta_1} \cdots p_s^{\beta_s}$, $c = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$ avec $\alpha_i, \beta_i, \gamma_i \geq 0$ et p_1, \dots, p_s les facteurs premiers distincts de a, b et c .

Par conséquent les décompositions de ca et cb sont

$$ca = \prod_{i=1}^n p_i^{\alpha_i + g_i}, \quad cb = \prod_{i=1}^n p_i^{\beta_i + g_i}, \quad \text{et qui entraîne}$$

$$\operatorname{pgcd}(ca, cb) = \prod_{i=1}^n p_i^{\min(\alpha_i + g_i, \beta_i + g_i)} = \prod_{i=1}^n p_i^{\alpha_i + \min(\alpha_i, \beta_i)}$$

car $\min(\alpha_i + g_i, \beta_i + g_i) = g_i + \min(\alpha_i, \beta_i)$ si $\{1, \alpha\}$,

en effet $\alpha_i + g_i \leq \beta_i + g_i$ si $\alpha_i \leq \beta_i$.

Alors $\operatorname{pgcd}(ca, cb) = \left(\prod_{i=1}^n p_i^{g_i} \right) \operatorname{pgcd}(a, b) = |c| \operatorname{pgcd}(a, b)$.

q2) En gardant les mêmes notations on a $a^2 = \prod_{i=1}^n p_i^{2\alpha_i}$, $b^2 = \prod_{i=1}^n p_i^{2\beta_i}$

$$\operatorname{pgcd}(a^2, b^2) = \prod_{i=1}^n p_i^{\min(2\alpha_i, 2\beta_i)} = \prod_{i=1}^n p_i^{2\min(\alpha_i, \beta_i)}$$

car $(\alpha_i \leq \beta_i \text{ ou } 2\alpha_i \leq 2\beta_i)$ donc $\min(2\alpha_i, 2\beta_i) \geq 2\min(\alpha_i, \beta_i)$.

Par conséquent $\operatorname{pgcd}(a^2, b^2) = \left(\prod_{i=1}^n p_i^{\min(\alpha_i, \beta_i)} \right)^2 = \operatorname{pgcd}(a, b)^2$.

q3) Si p est premier et $p \mid c$, puisque $p \mid a$ et $p \mid b$ donc $p \mid \operatorname{pgcd}(b, c)$
 Ceci est impossible donc aucun premier ne divise b et c à la fois
 d'où $\operatorname{pgcd}(b, c) = 1$.

q4) Si $\operatorname{pgcd}(a, bc) = 1$ alors d'après q3), on que $b \mid bc$ et $c \mid bc$
 on a $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(a, c) = 1$.

Si néanmoins $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(a, c) = 1$ et p est premier
 tel que $p \mid a$ et $p \mid bc$ alors, d'après le lemme d'Euclide,
 on a $p \mid b$ ou $p \mid c$. Or si $p \mid a$, $p \mid b$ on a $\operatorname{pgcd}(a, b) = 1$ d'où
 une contradiction et si $p \mid a$, $p \mid c$ on a $\operatorname{pgcd}(a, c) = 1$, ce qui est
 de nouveau contradictoire. Par conséquent aucun premier ne divise
 a et bc à la fois ce qui signifie exactement que
 $\operatorname{pgcd}(a, bc) = 1$.

95) Si $d \mid a+b$ et $d \mid a-b$ alors $d \mid a+b+a-b=2a$ et $d \mid (a+b)-(a-b)=2b$
 donc $d \mid \text{pgcd}(2a, 2b) = 2 \cdot \text{pgcd}(a, b) \geq 2$. Donc $d \geq 2$ ou $d \leq 2$ donc $\text{pgcd}(a+b, a-b) \leq 2$ (ou 1).
 (ex: $a=1, b=1, \text{pgcd}(2, 0)=2$ et $a=1, b=0, \text{pgcd}(1, 0)=1$). Si $d \nmid a+b$ et $d \nmid a-b$ avec p premier
 on a $p \nmid a+b$ et $p \nmid a-b$ ou $p \nmid a+b-b=2b$ donc $p \nmid \text{pgcd}(a, b)=1$.
 donc $\text{pgcd}(a+b, a-b)=1$

(ex 16) Si $d \mid n$ et $d \mid n+1$

on a $d \mid n+1-n=1$ donc $d \geq 1$ donc $\text{pgcd}(n, n+1)=1$.

Par conséquent $\text{ppcm}(n, n+1) = \frac{n(n+1)}{\text{pgcd}(n, n+1)} = n(n+1)$.

(ex 17)

91) On a $637 = 7^2 \times 13$ et $595 = 5 \times 7 \times 17$ donc

$$\text{pgcd}(637, 595) = 7,$$

On pourra effectuer aussi l'algorithme d'Euclide :

$$637 = 595 + 42$$

$$595 = 42 \times 14 + 7$$

avec un dernier reste non nul égal à 7.

$$42 = 6 \times 7 + 0$$

92) On a $637x + 595y = 91 = 7 \times 13$. On peut donc

dire que l'équation a des solutions, vu que $7 \mid 91$.

On doit, pour la seconde, trouver d'abord une solution particulière. Cette solution nous est fournie par les coefficients de Bézout soit pour 637 et 595 obtenus en remontant l'algorithme d'Euclide de la 91), soit pour $\frac{637}{7} = 91$ et

$\frac{595}{7} = 85$ premiers entre eux, vu que notre équation

est équivalente à l'équation $91x + 85y = 13$.

La première variation nous donne : $7 = 595 - 42 \times 14 =$
 $= 595 - (637 - 595) \times 14 = 637 \times (-14) + 595 \times 15$

d'où $7 \times 13 = 637 \times (-14 \cdot 13) + 595 \times (15 \cdot 13)$.

On pose $x_0 = -14 \cdot 13$, $y_0 = 15 \cdot 13$ et on obtient

$$637x + 595y = 637x_0 + 595y_0 \quad (=)$$

$637(x-x_0) = 595(y_0-y)$. (La ~~équivaut à~~ $91(x-x_0) = 25(y_0-y)$)

et comme $\text{pgcd}(91, 25) = 1$ on a $91 \mid y_0-y$ par le lemme de Gauss. On écrit alors
 $y_0-y = 91k$, avec $k \in \mathbb{Z}$. L'équation $637(x-x_0) = 25(y_0-y)$

devient $g_1(x - x_0) = 85 \cdot g_1 \cdot k \quad (\Rightarrow x - x_0 = 85k \Leftrightarrow)$
 $x = 85k + x_0.$

Posons $x = 85k + x_0$, $y = y_0 - g_1 k$ pour $k \in \mathbb{Z}$. Alors on a
 bien $637(85k + x_0) + 595(y_0 - g_1 k) = 637x_0 + 595y_0 = 91$
 donc les solutions de l'équation sont effectivement
 de la forme $x = 85k + x_0 = 85k + 14 \cdot 13$
 $y = y_0 - g_1 k = 15 \cdot 13 - g_1 k$ pour $k \in \mathbb{Z}$.

La deuxième variante consiste à écrire l'algorithme
 d'Euclide pour g_1 et 85 , donc à diviser par 7 l'algorithme
 d'Euclide de la q1) : $g_1 = 85 + 6$
 $85 = 6 \times 14 + \boxed{1}$
 $6 = 6 \times 1 + 0$ d'où

$$1 = 85 - 6 \times 14 = 85 - (g_1 - 85) \times 14 = 85 \cdot 15 - g_1 \cdot 14$$

Posons $13 = \underbrace{85 \cdot 13 \cdot 15}_{y_0} + \underbrace{g_1(-13 \cdot 14)}_{x_0}$ et $x_0 = -13 \cdot 14, y_0 = 13 \cdot 15$

On a $13 = g_1 x + 85 y = g_1 x_0 + 85 y_0 \Rightarrow$

$g_1(x - x_0) = 85(y_0 - y)$. On arrive à la même situation
 que ci-dessus donc aux mêmes solutions $\begin{cases} x = 85k + 14 \cdot 13 \\ y = 15 \cdot 13 - g_1 k, k \in \mathbb{Z} \end{cases}$

q3) On a $143 = 11 \cdot 13$ donc $7 \nmid 143$. On suit alors que cette
 équation n'a pas de solutions entières. En effet $7 \nmid 637x + 595y$
 si $x, y \in \mathbb{Z}$ donc $637x + 595y \neq 143$.

(ex 18) q1) On a 283 premier et $1722 = 2 \times 3 \times 7 \times 41$ donc
 $\text{pgcd}(1722, 283) = 1$ et $1/31$ donc cette équation
 admet des solutions dans \mathbb{Z} . On doit trouver d'abord
 une solution particulière, donc effectuer l'algorithme d'Euclide
 entre 1722 et 283 pour trouver une relation de Bézout du type
 $1722u + 283v = 1$.

$$\text{On a } 1722 = 283 \cdot 6 + 24$$

$$283 = 24 \cdot 11 + 19$$

$$24 = 19 + 5$$

$$19 = 5 \times 3 + 4$$

$$5 = 4 + 1 \quad \text{d'où}$$

$$1 = 5 - 4 = 5 - (19 - 5 \times 3) = 5 \times 4 - 19 = (24 - 19) \times 4 - 19 =$$

$$= 24 \times 4 - 19 \times 5 = 24 \times 4 - (283 - 24 \cdot 11) \cdot 5 =$$

$$= 24 \cdot 59 - 283 \cdot 5 = (1722 - 283 \cdot 6) \cdot 59 - 283 \cdot 5 =$$

$$= 1722 \cdot 59 - 283 \cdot 359 \quad \text{donc}$$

$$31 = \underbrace{1722 \cdot 59 \cdot 31}_{y_0} + 283 \underbrace{(-359 \cdot 31)}_{x_0} \quad \text{et on pose } x_0 = -359 \cdot 31 \\ y_0 = 59 \cdot 31$$

pour solution particulière.

$$\text{On voit que } 283x + 1722y = 283x_0 + 1722y_0 \quad (2)$$

$$283(x - x_0) = 1722(y_0 - y) \quad \text{donc on a que}$$

$\text{pgcd}(283, 1722) = 1$ on a $283 \mid y_0 - y$ d'après le lemme de

Gauss. D'où $y = y_0 - 283k$ pour $k \in \mathbb{Z}$ et

$$283(x - x_0) = 1722 \cdot 283 \cdot k \quad (2) \quad x - x_0 = 1722k$$

$$(2) \quad x = 1722k + x_0.$$

on obtient toutes les solutions en prenant $x = 1722k - 359 \cdot 31$

$$y = 59 \cdot 31 - 283k$$

pour $k \in \mathbb{Z}$.

$$92) \quad \text{On a } 365 = 72 \cdot 5 \text{ et } 72 = 2^3 \cdot 3^2 \text{ donc } \text{pgcd}(365, 72) = 1$$

et l'équation $365x + 72y = 18$ admet des solutions.

$$\text{On a } 365 = 72 \cdot 5 + 5$$

$$72 = 5 \times 14 + 2$$

$$5 = 2 \times 2 + 1 \quad \text{donc } 1 = 5 - 2 \times 2 = 5 - (72 - 5 \times 14) \times 2 =$$

$$= 5 \times 29 - 72 \times 2 = (365 - 72 \times 5) \times 29 - 72 \times 2 = 365 \times 29 - 72 \times 147$$

$$\text{et } 18 = 365 \times 29 + 18 + 72 \underbrace{(-147 \cdot 18)}_{y_0} = 365x + 72y. \quad \text{Alors}$$

$$365(x - x_0) = 72(y_0 - y) \quad \text{et comme } \text{pgcd}(365, 72) = 1 \text{ on a}$$

$$y_0 - y = 365k, \quad x - x_0 = 72k, \quad k \in \mathbb{Z}. \quad \text{Les solutions sont } x = 72k + 29 \cdot 18 \\ y = -147 \cdot 18 - 365k$$

93) On "prouve" que 101 est premier et $150 = 2 \times 3 \times 5^2$ donc

F1.13

$\text{pgcd}(101, 150) = 1$ et l'équation admet des solutions.

On écrit $150 = 101 \times 1 + 49$

$$101 = 49 \times 2 + 3$$

$$49 = 3 \times 16 + 1 \quad \text{donc } 1 = 49 - 3 \times 16 = 49 - (101 - 49 \times 2) \times 16 \\ = 49 \times 33 - 101 \times 16 = (150 - 101) \times 33 - 101 \times 16 = 150 \times 33 - 101 \times 49$$

Alors $15 = 101 \underbrace{(-49 \cdot 15)}_{x_0} + 150 \underbrace{33 \cdot 15}_{y_0} = 101x + 150y$ entraîne

$$101(x - x_0) = 150(y_0 - y) \quad \text{et comme } \text{pgcd}(101, 150) = 1 \text{ on a}$$

$$y_0 - y = 101k \quad \text{et} \quad x - x_0 = 150k \quad \text{pour } k \in \mathbb{Z}.$$

Les solutions sont $x = 150k - 49 \cdot 15$

$$y = 33 \cdot 15 - 101k \quad \text{pour } k \in \mathbb{Z}.$$

94) On a $282 = 2 \times 3 \times 47$ et $678 = 2 \times 3 \times 113$ donc

$\text{pgcd}(282, 678) = 6$. Comme $6 \mid 66$ l'équation a des solutions.

Elle s'écrit à $47x + 113y = 11$, on écrit

$$113 = 47 \times 2 + 19$$

$$47 = 19 \times 2 + 9$$

$$19 = 9 \times 2 + 1 \quad \text{donc } 1 = 19 - 9 \times 2 = 19 - (47 - 19 \times 2) \times 2 =$$

$$= 19 \times 5 - 47 \times 2 = (113 - 47 \times 2) \times 5 - 47 \times 2 = 113 \times 5 - 47 \times 12$$

$$\text{d'où } 11 = 47 \underbrace{(-12 \cdot 11)}_{x_0} + 113 \underbrace{(5 \cdot 11)}_{y_0} = 47x + 113y \quad \text{Comme } 47(x - x_0) \\ = 113(y_0 - y)$$

et que $\text{pgcd}(47, 113) = 1$ on a $y_0 - y = 47k$

$$x - x_0 = 113k \quad \text{pour } k \in \mathbb{Z} \quad \text{donc les solutions}$$

recherchées sont $x = 113k - 12 \cdot 11 = 113k - 132$

$$y = 55 - 47k \quad , \quad k \in \mathbb{Z}.$$

(ex 19) Si $\text{pgcd}(a, b) = 12$ on a que $a = 12a'$, $b = 12b'$ avec

$\text{pgcd}(a', b') = 1$. Alors $\text{ppcm}(a, b) = 12a'b' = 360$

donc $a'b' = 30$. Par conséquent $(a', b') \in \{(1, 30), (2, 15), (3, 10),$

$(5, 6), (6, 5), (10, 3), (15, 2), (30, 1)\}$ et $(a, b) \in \{(12, 360), (24, 180), (36, 120),$

$(60, 72), (72, 60), (120, 36), (180, 24), (360, 12)\}$.

(ex 20) a) On a $a = 2a'$
 $b = 9b'$ avec $\text{pgcd}(a', b') = 1$ et
 $g(a' + b') = 360$ donc $a' + b' = 40$.

Par conséquent $(a', b') \in \{(1, 39), (3, 37), (7, 33), (9, 31), (11, 29), (13, 27), (17, 23), (19, 21), (21, 19), (23, 17), (27, 11), (29, 11), (31, 9), (33, 7), (37, 3), (39, 1)\}$
et $(a, b) = g(a', b') = (9a', 9b')$.

b) Si $a = 18a'$
 $b = 18b'$ avec $\text{pgcd}(a', b') = 1$ on a $18^2 a' b' = 1620 = 18^2 \cdot 5$

donc $a' b' = 5$ et $(a', b') \in \{(1, 5), (5, 1)\}$ donc $(a, b) \in \{(18, 90), (90, 18)\}$

(ex 21) q1) On a $16 = 7 \times 2 + 2$
 $7 = 2 \times 3 + 1$ donc $1 = 7 - 2 \times 3 = 7 - (16 - 7 \times 2) \times 3 =$
 $= 7 \times 7 - 16 \times 3 = 7 \times 7 + 16(-3)$ et on peut prendre pour
solution particulière $x_0 = 7, y_0 = -3$.

q2) On a $7x_0 + 16y_0 = 7x + 16y \Leftrightarrow 7(x - x_0) = 16(y_0 - y)$.

Comme $\text{pgcd}(7, 16) = 1$ cela entraîne $y_0 - y = 7k$
 $x - x_0 = 16k$ pour $k \in \mathbb{Z}$
donc les solutions recherchées sont $x = 16k + 7$
 $y = -3 - 7k$ pour $k \in \mathbb{Z}$

q3) a) Si Alice possède un grand récipient en plus de ses deux récipients, elle peut juste mettre 7 fois 7 l dans ce grand récipient, et ensuite elle verse 3 fois 16 l dans 49 l du grand récipient pour arriver à 1 l car $7 \times 7 - 16 \cdot 3 = 1$.
Le problème ne suppose pas l'existence d'un grand récipient donc on va suivre cette procédure sans utiliser de grand récipient mais en remplissant 7 fois le récipient de 7 l et on le vidant petit à petit dans le récipient de 16 l (qui sera vidé 3 fois) pour aboutir à 1 l.

On fait un tableau qui montre les étapes nécessaires de notre procédé :

Volume de liquide dans le récipient de 16 l à chaque étape	0 7 7 14 14 16 0 5 5 12 12 16 0 3 3 10 10 16
Volume de liquide dans le récipient de 7 l à chaque étape	7 0 7 0 7 5 5 0 7 0 7 3 3 0 7 0 7 1

On a utilisé 49 l d'eau et le récipient de 16 l a été rempli 3 fois (et vidé 2 fois)

On peut aussi utiliser la solution pour $k = -1$, qui correspond à $x = -9, y = 4$ et à la formule $16 \cdot 4 - 7 \cdot 9 = 1$ et au tableau

Volume de liquide dans le récipient de 16 l	16 9 9 2 2 0 16 11 11 4 4 0 16 12 12 6 6 0 16 15 15 8
Volume de liquide dans le récipient de 7 l	0 7 0 7 0 2 2 2 0 7 0 4 4 7 0 7 0 6 6 7 0 7

On a utilisé $16 \cdot 4 = 64$ l d'eau et le récipient de 16 l a été rempli 4 fois

b) On cherche donc une solution de l'équation avec y munie d'un valeur absolue, jusqu'à $y = -7k - 3$ cette solution correspond à $k = 0, y = -3$ qui a été décrite ci-dessus.

94) Alice ne peut pas obtenir 12 l d'eau avec des récipients de 14 l et de 21 l car à chaque opération elle obtient une quantité de liquide qui correspond à α l avec α multiple de 7 ! En effet $\alpha = 21x + 14y$ est toujours un multiple de 7 pour $x, y \in \mathbb{Z}$.

(ex22)

Considérons

$$\alpha_1 = (n+1)! + 2, \alpha_2 = (n+1)! + 3, \dots, \alpha_m = (n+1)! + (n+1) \text{ pour } n \geq 1$$

On a $2 | \alpha_1, 3 | \alpha_2, \dots, n+1 | \alpha_m$ et $\alpha_m = (n+1)(n! + 1) > n+1$

En général $\alpha_i = (i+1) \left[\frac{(n+1)!}{i+1} + 1 \right] > i+1$ pour $1 \leq i \leq m$ donc α_i n'est pas premier.

(ex23)

On écrit $11p+1 \equiv k^2$ pour $k \in \mathbb{Z}$. Les racines de k^2 modulo 11

peuvent être que $0, \pm 1, \pm 2, \pm 3, \pm 4$ ou ± 5 et pour chacun de ces cas

les racines de k^2 modulo 11 sont $0, 1, 4, 9, 5$ ou 3 . Par conséquent, pour que $k^2 = 11p+1$ on a nécessairement $k = 11k' \pm 1$ et $k^2 = 121k'^2 \pm 22k' + 1$

avec $k' \in \mathbb{Z}$. Alors $11p = 121k'^2 \pm 22k' \Leftrightarrow p = 11k'^2 \pm 2k' = k'(11k' \pm 2)$

Or que p est premier et que $11k' \pm 2 \neq \pm 1$ on doit avoir $k' = \pm 1$

Pour $k' = -1$ on a $k = -12$ ou $k = -10$ donc $p = 13$ qui convient ou $p = 9$ qui ne convient pas.

Pour $k' = 1$ on a $k = 12$ ou $k = 10$ donc toujours $p = 13$ premier ou $p = 9$ qui n'est pas premier. La seule possibilité avec p premier et par conséquent $p = 13$

(ex24)

Puisque a et b sont premiers entre eux, leurs décompositions en facteurs premiers sont $a = \pm p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ et $b = \pm p_{t+1}^{\beta_{t+1}} \cdots p_s^{\beta_s}$ avec $\alpha_i > 0$ et p_1, \dots, p_s des premiers distincts.

Par conséquent la décomposition en facteurs premiers de $a b = c^2$

est $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_{t+1}^{\beta_{t+1}} \cdots p_s^{\beta_s}$ et a et b ont de même signe.

Comme il s'agit de la décomposition en facteurs premiers d'un carré, on a $\alpha_i = 2\gamma_i$ pour tout i compris entre 1 et t .

On conclut facilement que $a = \pm p_1^{2\gamma_1} \cdots p_t^{2\gamma_t}$ et

$b = \pm p_{t+1}^{2\beta_{t+1}} \cdots p_s^{2\beta_s}$ sont donc tous deux de même signe.

(ex25)

On a $b \geq 2$ et $1010_B = b^4 + b^2 + 1 = b^4 + 2b^2 + 1 - b^2 = (b^2 + 1)^2 - b^2 = (b^2 + b + 1)(b^2 - b + 1)$, les deux facteurs étant strictement supérieurs à 1 on a donc que 1010_B n'est pas un nombre premier.

ex 26

Les notes de ~~l'addition~~ modulo 7 sont $0, \pm 1, \pm 2$ ou ± 3 donc les notes de ~~l'addition~~ de m^2 modulo 7 sont $0, 1, 4$ ou 2 et les notes de ~~l'addition~~ de m^3 modulo 7 sont $0, \pm 1, \pm 1$ ou ± 1 . Si n est à la fois un carré et un cube, ses notes pour ~~l'addition~~ modulo 7 ne peuvent être que 0 ou 1 donc $\exists k \in \mathbb{N}$ tel que $n = 7k$ ou $7k+1$.

Voir la remarque après l'exercice 27 pour une autre solution.

ex 27

$$\text{q1) On écrit } 25 = 9 \times 2 + 7$$

$$9 = 7 \times 1 + 2$$

$$7 = 2 \times 3 + 1$$

$$\text{donc } 1 = 7 - 2 \times 3 = 7 - (9 - 7) \times 3 = \\ = 7 \times 4 - 9 \times 3 = (25 - 9 \times 2) \times 4 - 9 \times 3 = \\ = 25 \times 4 - 9 \times 11$$

et on peut considérer $u=4$, $v=-11$.

$$\text{q2) On a } c^{25} = a^{25u} b^{25v} = a^{1-9v} (b^{25})^v = a \cdot a^{-9v} a^v = a \text{ et}$$

$$c^9 = a^9 u b^{9v} = b^{25u+9v} = b$$

q3) Écrivons x sous forme de fraction simplifiée, $x = \frac{p}{t}$ avec $s, t \in \mathbb{Z}$

$$\text{pgcd}(s, t) = 1. \text{ Alors si } x = \frac{s^k}{t^k} = m \in \mathbb{Z} \text{ on a } mt^k = s^k.$$

Si $t \neq \pm 1$ alors s n'a pas de facteur premier de t . On a $p \mid s^k$ donc plus par le lemme d'Euclide, $\text{pgcd}(s, t) \neq 1$ et cela contredit

l'existence de p . Par conséquent $t = \pm 1$ et $x \in \mathbb{Z}$.

q4) A priori $c \in \mathbb{Q}$ puisque u ou v est négatif. Mais comme $c^{25} = a \in \mathbb{N}$,

d'après la q3) on a $c \in \mathbb{Z}$. On a aussi c non nul car a non nul, et c positif car a positif donc $c \in \mathbb{N}^*$. On aurait pu utiliser également $c^9 = b \in \mathbb{N}$ pour aboutir aux mêmes conclusions.

q5) D'après le théorème de Bézout on sait qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $mu + nv = 1$, pour $c = a^u b^v$ on a

$$c^m = a^{mu} b^{mv} = a^{nu} a^{mv} = a \text{ et } c^n = a^{mu} b^{nv} = b^{nu+mv} = b$$

A priori $c \in \mathbb{Q}$ mais comme $c^m = a \in \mathbb{N}^*$ on a (d'après q3) que $c \in \mathbb{Z}$ et $c \neq 0$. Si n est pair, m est impair car $\text{pgcd}(m, n) = 1$ donc $b^n = b > 0$ nous aide à conclure que $c \in \mathbb{N}^*$. Si n impair on a $c^n = a > 0$ donc de nouveau $c \in \mathbb{N}^*$. Dans tous les cas $c \in \mathbb{N}^*$.

pour cet exercice on pourra utiliser aussi la décomposition en facteurs premiers de a et de b :

$$\text{Si } a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

$b = p_1^{\beta_1} \cdots p_n^{\beta_n}$ avec $\alpha_i > 0, \beta_i > 0$ et p_i les facteurs premiers de a et de b alors la décomposition de

$$x = a^m = b^n \text{ et } \prod_{i=1}^{n \alpha_i} p_i = \prod_{i=1}^n p_i^{\alpha_i} = x \text{ et par suite}$$

on a $m \alpha_i = n \beta_i \forall i \in \{1, \dots, n\}$. Or $m \mid n \beta_i$ et $\text{pgcd}(m, n) = 1$ implique par le lemme de Gauss que $m \mid \beta_i, \forall i$.

De même $m \mid m \alpha_i \forall i$ et $\text{pgcd}(m, n) = 1$ implique que $n \mid \alpha_i, \forall i$.

Donc $\alpha_i = n \alpha'_i$, $\beta_i = m \beta'_i$ et $m n \alpha'_i = m n \beta'_i$ donc $\alpha'_i = \beta'_i$.

$$\text{Alors } a = \left(\prod_{i=1}^n p_i^{\alpha'_i} \right)^m = c^m \text{ pour } c = \prod_{i=1}^n p_i^{\alpha'_i} \text{ et}$$

$$b = \left(\prod_{i=1}^n p_i^{\alpha'_i} \right)^n = c^n \quad \text{et } c \in \mathbb{N}^*.$$

Remarque. Cet exercice et le petit théorème de Fermat ($x^{p-1} \equiv 1 \pmod{p}$ si p premier)

nos permettent de reprendre d'une autre manière l'exercice 26 :
Comme $n = a^2 = b^3$ et que $\text{pgcd}(2, 3) = 1$ on a que $a = c^3 / \text{et } b = c^2 /$
donc $n = c^6$. Si $7 \mid c$ alors $7 \mid c^6 = n$ donc $n = 7k$ pour $k \in \mathbb{N}$.

Si $7 \nmid c$ on applique le petit théorème de Fermat avec $p = 7$ premier. Donc $n = c^{7-1} = c^6 \equiv 1 \pmod{7}$ d'où $n = 7k+1$ pour $k \in \mathbb{N}$.