► ► 14 : ARITHMÉTIQUE

Pratique 1 :

1. 2 divise 6 et non l'inverse, 6 est multiple de 2, car $6 = 2 \times 3$. 3 ne divise pas 8, ni l'inverse.
Seuls 1 et -1 divisent tous les entiers : pour tout k dans $\mathbb{Z}$, $k = 1 \times k = (-1) \times (-k)$ et inversement seuls 1 et -1 divisent 1.

2. $\text{div}(0) = \mathbb{Z}$ puisque pour tout k dans $\mathbb{Z}$ on a : $0 = k \times 0$. Enfin, $\text{div}(6) = \{1; 2; 3; 6; -1; -2; -3; -6\}$.

1►

∗ *Preuve* : 1) Soit p, q et r trois naturels.
- $|$ est réflexive puisque tout entier divise lui-même : $p = p \times 1$
- $|$ est symétrique : si $p|q$ et $q|p$, alors il existe deux naturels m et n tels que $q = p \times m$ et $p = q \times n$ d'où $pq = (pq) \times (mn)$ donc $mn = 1$ (ou $p = q = 0$ car 0 ne divise que 0).
- $|$ est transitive : si $p|q$ et $q|r$, alors il existe deux naturels m et n tels que $q = m \times p$ et $r = n \times q$, donc $r = (mn) \times p$, donc p divise r.

3) Pour des naturels a, b et k, si $a = b \times k$ alors $|a| = |b||k|$ avec $|k| \geqslant 1$ donc $|a| \geqslant |b|$.

4) Toutes les lettres désignant des entiers relatifs, si $b = a \times m$ et $c = a \times n$, alors $ub + vc = (um + vn) \times a$, d'où le résultat.

5) De même, si $c = am$ et $d = bn$, alors $cd = (ab) \times (mn)$ donc ab divise cd. □

∗ Avec le point 2, on voit que 0 est le plus grand élément dans $\mathbb{N}$ muni de la relation d'ordre $|$.

∗ Attention aux propositions inverses : si a divise $b + c$, on ne sait rien entre a et b ou c. Par exemple, 2 divise $3 + 5$ sans diviser ni 5 ni 3...
De même, si a et b divisent c, ab ne divise pas forcément c. Par exemple, 2 et 2 divisent 2, mais 4 ne divise pas 2 ; 3 et 6 divisent 12, mais 18 ne divise pas 12.
On doit pouvoir mieux faire...

2►

∗ Par exemple : $6 = 2 \times 3 + 0$, $19 = 4 \times 4 + 3$, $-19 = 4 \times (-5) + 1$.

∗ *Preuve* : Si $a \geqslant 0$, on retranche b à a et on recommence jusqu'à obtenir le reste r avec $0 \leqslant r < b$. Plus rigoureusement, $\{c \in \mathbb{N} \mid a - bc \geqslant 0\}$ est une partie de $\mathbb{N}$ non vide (elle contient 0) et majorée par a, donc elle admet un plus grand élément, noté q. Alors $a - bq$ est positif et inférieur ou égal à $b - 1$ sans quoi $q + 1$ appartient à l'ensemble. On a : $a = bq + r$ avec $0 \leqslant r < b$.
Si $a < 0$, on ajoute de même b à a et on recommence jusqu'à obtenir le reste r avec $0 \leqslant r < b$. Plus rigoureusement, $\{c \in \mathbb{N} \mid a + bc \geqslant 0\}$ est une partie de $\mathbb{N}$ non vide (elle contient $-a$), donc elle admet un plus petit élément, noté $-q$. Alors $a - bq = a + b \times (-q)$ est positif est inférieur strictement à b sans quoi $-q - 1$ appartient à l'ensemble. On a $a = b(-q) + r$ avec $0 \leqslant r < b$.
Ceci prouve l'existence de la division euclidienne.

Supposons $a = bq + r = bq' + r'$ avec les conditions imposées. Alors : $b(q - q') = r' - r$ donc $|q' - q| < 1$ puisque $|r' - r| < b$. Comme q et q' sont des entiers relatifs, ils sont égaux, donc $q = q'$ et $r = r'$. □

∗ Informatiquement, une soustraction est moins coûteuse qu'une division, les interprétations (en début de preuve) en terme de soustractions peuvent être utiles...

3►

∗ *Preuve* : Par récurrence sur n, on montre le résultat d'existence P_n pour $a \in [\![b^n, b^{n+1} - 1]\!]$.
Pour $n = 0$, donc $a \in [\![1, b - 1]\!]$, c'est clair : $a = ab^0$.
Soit n un naturel non nul, on suppose que pour tout $k \leqslant n - 1$, P_k est vraie. Soit $a \in [\![b^n, b^{n+1} - 1]\!]$. La division euclidienne de a par b^n s'écrit : $a = b^n a_n + a'$ avec $a_n \neq 0$ et $a' \leqslant b^n - 1$. Par hypothèse de récurrence, puisque a' appartient à un intervalle de forme $[\![b^k, b^{k+1} - 1]\!]$, a' peut s'écrire $\sum_{k=0}^{n-1} a_k b^k$ (sans savoir si $a_{n-1} \neq 0$). Finalement, $a = \sum_{k=0}^{n} a_k b^k$ avec $a_n \neq 0$, et P_n est vraie. On conclut par le principe de récurrence.

Supposons maintenant deux décompositions distinctes : $a = \sum_{k=0}^{n} a_k b^k = \sum_{k=0}^{n} a'_k b^k$. Soit p le plus grand indice tel que $a_p \neq a'_p$. Posons $c = \sum_{k=0}^{p} a_k b^k = \sum_{k=0}^{p} a'_k b^k$ avec $a_p \neq a'_p$. Or le quotient de la division euclidienne de c par b^p est $a_p = a'_p$, car $0 \leqslant \sum_{k=0}^{p-1} a_k b^k \leqslant \sum_{k=0}^{p-1} (b-1)b^k = b^p - 1$. Par unicité de la division euclidienne, on aboutit à une contradiction. □

∗ On obtient les cœfficients successifs de a

i) pour une lecture de gauche à droite, par divisions euclidiennes successives par b^k des restes successifs, k variant de n à 0, et en lisant les quotients successifs (mais cela nécessite de connaître l'intervalle $[\![b^n, b^{n+1} - 1]\!]$ contenant a), ou

ii) pour une lecture de droite à gauche, en lisant les restes successifs et divisant les quotients successifs par b jusqu'au premier quotient nul.

Par exemple :

i) $14 = 8 \times 1 + 6$, puis $6 = 4 \times 1 + 2$, puis $2 = 2 \times 1 + 0$, et par les quotients :

$$14 = 2^3 \times 1 + 2^2 \times 1 + 2 \times 1 + 0 = \overline{1110}^2$$

ii) $14 = 2 \times 7 + 0$, puis $7 = 2 \times 3 + 1$, puis $3 = 2 \times 1 + 1$ puis $1 = 2 \times 0 + 1$, et par les restes,

$$14 = 0 + 2 \times 1 + 2^2 \times 1 + 2^3 \times 1 = \overline{1110}^2$$

∗ En base 10, c'est la notation habituelle. En base inférieure à 10, on utilise les caractères habituels. Sinon, on utilise des lettres pour les caractères manquants.

Par exemple, en base 16, le nombre écrit 252 en base 10 s'écrit : $\overline{FC}^{16}$, puisque $252 = 16 \times 15 + 12$ et $15 = 16 \times 0 + 15$.

Pratique 2 :

$19 = \overline{201}^3$, $\overline{141}^5 = 1 + 4 \times 5 + 1 \times 5^2 = 46$, et $390 = \overline{186}^{16}$.

4►

∗ Se rappeler que les p_i valent 0 ou 1.

∗ $p = O(2^n)$, la complexité de la méthode est donc logarithmique (suivant p).

5►

∗ *Preuve* : 1) $n|a$ signifie que n divise $a - 0$, donc $a \equiv 0\ [n]$.

2) Soit a, b, et c des entiers.
- $a - a = 0$ est divisible par n donc $a \equiv a\ [n]$.
- si $a - b$ est divisible par n, alors $b - a$ l'est aussi.
- supposons $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $b - a$ et $c - b$ sont divisibles par n, donc $(c - b) - (b - a)$ l'est aussi, soit $a \equiv c\ [n]$.

Supposons $a \equiv b\ [n]$ et posons $a = nq + r$ et $b = nq' + r'$ les divisions euclidiennes de a et b par n. Alors $b - a = n(q - q') + (r - r')$ est divisible par n si, et seulement si, $r = r'$ puisque $0 \leqslant |r - r'| < n$.

3) et 4) Découlent des propriétés déjà vues de divisibilité.

5) S'il existe un entier k tel que $b - a = kn$, alors $mb - ma = k(mn)$. Inversement, m étant non nul, l'inverse est vrai. □

∗ On a donc tout intérêt à calculer les congruences des premières puissances pour calculer celles des puissances plus grandes ...

Pratique 3 :

1. $2 \equiv -1$ [3] donc $2^{355} \equiv (-1)^{355}$ [3], le résultat est donc 2.

2. Soit $n = 2p + 1$ un entier relatif impair. Alors : $n^2 = 4p^2 + 4p + 1 = 4p(p + 1) + 1$.
Or $p(p + 1)$ est toujours pair, donc $4p(p + 1)$ est toujours multiple de 8.

6►

On vérifiera plus loin que, pour deux entiers relatifs a et b, $pgcd(a, b)$ est le plus grand élément, au sens de la relation d'ordre de la divisibilité ($|$) dans $\mathbb{N}$, de l'ensemble des diviseurs naturels communs à a et b, ce qui justifie le choix $pgcd(0, 0) = 0$.

Pratique 4 :

1. $2 \wedge 8 = 2$, $12 \wedge (-18) = 12 \wedge 18 = 6$, $14 \wedge 22 = \text{Max}(\{1; 2; 7; 14\} \cap \{1; 2; 11; 22\}) = 2$.

2. Puisque $\text{div}(a) = \text{div}(|a|)$ et que l'intersection est commutative.

7►

Preuve : Soit a, b et q des entiers. Si k divise a et b, alors k divise $a - bq$ et b. Inversement, si k divise $a - bq$ et b, alors il divise $a - bq + bq = a$ et b. Les ensembles de diviseurs de a et b d'une part, et de $a - bq$ et b d'autre part, sont les mêmes, donc les deux pgcd sont les mêmes.

Si q est maintenant le quotient dans la division euclidienne de a par b, le reste est $r = a - bq$ et on obtient $a \wedge b = b \wedge r$. □

Intérêt : on va pouvoir itérer le procédé, avec une suite de restes à valeurs naturelles d'abord strictement décroissante tant qu'elle ne prend pas la valeur 0, donc nulle à partir d'un certain rang !

8►

C'est l'**algorithme d'Euclide** qui permet un calcul systématique du pgcd de deux entiers.
Notez qu'on a aussi $a \wedge b = b \wedge (a - b)$, ce qui permet une implémentation à base de soustractions, correspondant à l'autre implémentation de la division euclidenne, à base de soustractions.

9►

$*$ Attention : si (u, v) est un couple de Bezout associé à a et b, c'est-à-dire si $a \wedge b = au + bv$, alors pour tout entier c on a aussi $c(a \wedge b) = a(cu) + b(cv)$. On voit qu'un entier de type $au' + bv'$, qui est bien divisible par $a \wedge b$, n'est pas forcément égal à $a \wedge b$! On aura (presque) cette réciproque dans le cas particulier où $a \wedge b = 1$.

$*$ Plusieurs couples de Bezout peuvent être associés à a et b : par exemple, $1 = -2 + 3$ et $1 = 2 \times 2 - 3$, donc $(-1, 1)$ et $(2, -1)$ sont deux couples de Bezout associés à $a = 2$ et $b = 3$, dont le pgcd est 1.

$*$ *Preuve* : En appliquant l'algorithme d'Euclide, on construit une suite finie de restes :
$a = bq_1 + r_2$ soit $r_0 = r_1q_1 + r_2$, $r_1 = r_2q_2 + r_3$, etc., $r_{k-2} = r_{k-1}q_{k-1} + r_k$ avec $r_k = 0$ et $a \wedge b = r_{k-1}$ (dernier reste non nul).
On va fabriquer deux nouvelles suites en posant $u_0 = 1$ et $u_1 = 0$ d'une part, $v_0 = 0$ et $v_1 = 1$ d'autre part, puis pour $0 \leqslant n \leqslant k$: $u_{n-2} = u_{n-1}q_{n-1} + u_n$ et $v_{n-2} = v_{n-1}q_{n-1} + v_n$ (on calque les relations vérifiées par les restes), ce qui les définit parfaitement.
On a alors : $au_0 + bv_0 = a = r_0$, $au_1 + bv_1 = b = r_1$, $au_2 + bv_2 = a(u_0 - u_1q_1) + b(v_0 - v_1q_1) = r_0 - r_1q_1 = r_2$, et par récurrence, pour $0 \leqslant n \leqslant k$, $au_n + bv_n = r_n$.

Ce calcul constitue l'algorithme d'Euclide étendu : il permet le calcul effectif (et l'implémentation informatique de la détermination) d'un couple de Bezout associé à a et b, et en prouve l'existence puisqu'on obtient $a \wedge b = r_{k-1} = au_{k-1} + bv_{k-1}$. □

Pratique 5 :

On applique l'algorithme d'Euclide. Il y a peu d'étape, donc on peut "remonter" le calcul pour obtenir un couple de Bezout.

(a) $50 = 28 \times 1 + 22$, puis (b) $28 = 22 \times 1 + 6$, puis (c) $22 = 6 \times 3 + 4$, puis (d) $6 = 4 \times 1 + 2$, enfin $4 = 2 \times 2 + 0$. Donc $50 \wedge 28 = 2$ (dernier reste non nul).

On remonte les calculs : avec (d), $2 = 28 \wedge 50 = 6 - 4$.

Avec (b) et (c) : $2 = (28-22)-(22-3\times6) = 28-22\times2+6\times3 = 28-22\times2+28\times3-22\times3 = 28\times4-22\times5$.

Enfin, avec (a) : $a \wedge b = 28 \times 4 - (50 - 28) \times 5 = 28 \times 9 - 50 \times 5$, donc $(-5, 9)$ est un couple de Bezout associé à 50 et 28.

10►

$*$ *Preuve* : 1) et 2) ont déjà été vus.

Pour 3), il suffit d'appliquer l'algorithme d'Euclide à a et b en multipliant par c chaque opérations.

Pour 4) : Si k divise $a \wedge b$, alors il divise a et b puisqu'un diviseur d'un diviseur de n est un diviseur de n. Ceci montre l'inclusion de droite à gauche.
Pour l'inclusion directe, on utilise l'identité de Bezout : il existe u et v entiers tels que $a \wedge b = au + bv$, et on voit qu'un diviseur commun à a et b divise $a \wedge b$.

Pour 5) : puisque $\mathrm{div}((a \wedge b) \wedge c) = \mathrm{div}(a) \cap \mathrm{div}(b) \cap \mathrm{div}(c)$, expression symétrique suivant les lettres a, b et c, puisque l'intersection est commutative et associative.

$*$ La propriété 4) est intéressante ! Elle montre que $a \wedge b$ est la borne inférieure de l'ensemble $\{|a|; |b|\}$ dans l'ensemble ordonné $(\mathbb{N}, |)$, c'est-à-dire le plus grand élément de l'ensemble des minorants communs à a et b.

11►

Preuve : Soit a et b dans $\mathbb{Z}$.
Si $a = b = 0$, le résultat est clair puisque $a \wedge b = 0$, on peut choisir $a' = b' = 1$.
Sinon, $a \wedge b$ divise a et b : il existe a' et b' entiers relatifs tels que $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$. Il existe par ailleurs un couple (u, v) de Bezout associé à a et b : $a \wedge b = au + bv = (a \wedge b)(a'u + b'v)$. Comme $a \wedge b$ n'est pas nul, il reste $a'u + b'v = 1$, où l'on voit qu'un diviseur commun c à a' et b' vérifie $|c| = 1$.
Ainsi $a' \wedge b' = 1$. □

12►

$*$ Si r est un rationnel, il s'écrit comme quotient de deux entiers relatifs a et b non nul : $r = a/b$. En simplifiant par $a \wedge b$ et en utilisant le théorème précédent, on obtient une forme irréductible de r.

$*$ *Preuve du théorème de Bezout* : la partie directe vient de l'identité de Bezout pour deux entiers premiers entre eux ; pour la réciproque, déjà vue en fin du point précédent, si c divise a et b tels que $au + bv = 1$, alors c divise 1, donc $c = \pm1$, ce qui signifie que $a \wedge b = 1$. □

$*$ Cette équivalence du théorème de Bezout apporte une réciproque partielle à la proposition liée à l'identité de Bezout : pour a et b entiers, il existe u et v tels que $au + bv = a \wedge b$. Inversement, si on dispose d'une égalité de type $au + bv = d$, alors d n'a pas de raison d'être le pgcd de a et b, sauf dans le cas où $d = 1$.

$*$ On peut interpréter le théorème de Bezout en termes de congruences :

a et b sont premiers entre eux si, et seulement si, a est inversible modulo b

au sens où il existe un entier u tel que $au \equiv 1$ $[b]$. En effet, cette relation signfie que $au - 1$ est divisible par b, c'est-à-dire qu'il existe un entier v tel que $au - 1 = bv$, ou encore $au - bv = 1$ (relation de Bezout).

Par exemple : 4 est l'inverse de 2 modulo 7 puisque $2 \times 4 = 8 \equiv 1$ [7].

L'équation "modulaire" d'inconnue x : $2x \equiv 3$ [7] admet donc pour solutions les x tels que $x \equiv 5$ [7] (puisque $4 \times 3 = 12 \equiv 5$ [7]), c'est-à-dire les entiers s'écrivant $5 + 7k$ pour $k \in \mathbb{Z}$.

Ce type d'équation "linéaire" est plus difficile à résoudre lorsque le coefficient de x n'est pas inversible ! Par exemple, $2x \equiv 0$ [4] admet pour solutions les entiers pairs (et non pas les multiples de 4, on n'a pas pu "simplifier" par 2 qui n'est pas inversible modulo 4), et $2x \equiv 1$ [4] est une équation sans solution.

13►

∗ *Preuve* : Supposons a premier avec b : il existe un couple (u, v) de Bezout associé à a et b, soit $au + bv = 1$. D'où : $acu + bcv = c$. On voit donc que a, qui divise acu et bc, divise également c. □

∗ En terme de congruences : si $bc \equiv 0\ [a]$, et si $a \wedge b = 1$, alors $c \equiv 0\ [a]$. Mais on s'en doute puisque, comme on l'a vu, $a \wedge b = 1$ implique b inversible modulo a : en multipliant la première identité par l'inverse de b, il reste bien $c \equiv 0\ [a]$.

∗ Sans l'hypothèse $a \wedge b = 1$, on perd bien sûr la conclusion du théorème. Par exemple, 2 divise $6 = 2 \times 3$ sans être premier avec 2, et 2 ne divise pas 3... En termes de congruences, 2 n'est pas inversible modulo 6, $2 \times 3 \equiv 0\ [6]$ n'implique pas $3 \equiv 0\ [6]$!

14►

∗ *Preuve* : Par hypothèse, il existe a' et b' entiers tels que $aa' = c$ et $bb' = c$, donc $aa' = bb'$. Comme $a \wedge b = 1$, par le théorème de Gauss, a divise b' : il existe k entier tel que $b' = ak$. On en déduit : $c = abk$, c'est-à-dire que ab divise c. □

∗ On savait déjà la chose suivante : si ab divise c, alors a et b divisent c. La proposition donne donc une réciproque partielle dans le cas où a et b sont premiers entre eux.

15►

∗ *Preuve* : Soit d un diviseur commun à a et à bc : il existe k et l entiers tels que $a = dk$ et $bc = dl$. On obtient $bck = al$. Comme a est premier avec b, d'après le théorème de Gauss, a divise ck. De même, comme a est premier avec c, il divise k. Comme a divise k et k divise a, il vient $d = \pm 1$, ce qui montre que a et bc sont premiers entre eux. □

∗ En termes de congruences : le produit de deux inversibles modulo a est un inversible modulo a. L'inverse de ce produit est d'ailleurs le produit de ces inverses.

Pratique 6 :

Après division par $2 = 4 \wedge 10$, il reste : $2x - 5y = 2$.
2 et 5 sont premiers entre eux, et vérifient la relation de Bezout : $5 \times 1 - 2 \times 2 = 1$, d'où : $5 \times 2 - 2 \times 4 = 2$.
On a donc une solution particulière $(x_0, y_0) = (-4, -2)$.
Pour toute autre solution (x, y) : $2x - 5y = 2$ et $2x_0 - 5y_0 = 2$ donc $2(x - x_0) = 5(y - y_0)$. Par le théorème de Gauss, il existe k entier tel que $x - x_0 = 5k$ et $y - y_0 = 2k$, et réciproquement.
L'ensemble des solutions (x, y) est donné par les $(-4 + 5k, -2 + 2k)$, pour $k \in \mathbb{Z}$.

Pratique 7 :

Le butin B vérifie $B \equiv 3\ [16]$. Par ailleurs, $B \equiv 4\ [7]$ après la deuxième étape... Il s'agit donc de calculer B.
Comme 7 et 16 sont premiers entre eux, il existe u et v tels que $16u + 7v = 1$, c'est-à-dire que $16u \equiv 1\ [7]$ et $7v \equiv 1\ [16]$. Par conséquent, $B_0 = 16u \times 4 + 7v \times 3$ est une solution.
Or les u et v possibles sont donnés grâce au paragraphe précédent par les couples $(4 + 7k, -9 - 16k)$, $k \in \mathbb{Z}$, donc les gains possibles sont : $16 \times 4 \times 4 - 7 \times 9 \times 3 + 16 \times 7 \times k$ pour $k \in \mathbb{Z}$.
Au minimum, le cuisinier (chinois !) peut donc espérer un gain de $67 + 0 = 67$ pièces.

16►

Pour a et b entiers non nuls, $a \vee b$ est bien défini puisque l'ensemble des multiples strictement positifs communs à a et b contient $|a||b|$ et est minoré par 0.

Pratique 8 :

$12 \vee 3 = 12$, $(-10) \vee 15 = 10 \vee 15 = 30$, et $6 \vee (-5) = 6 \vee 5 = 30$.

17►

$*$ *Preuve* : Soit a, b et c strictement positifs (résultats clairs si l'un des entiers est nul).

1) Clair.

2) et 3) On peut écrire $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$ avec a' et b' premiers entre eux, donc $(a \wedge b)a'b'$ est un multiple commun à a et b. Inversement, si $c = ap = bq$ est un multiple commun à a et à b, alors $a'p = b'q$, et par le théorème de Gauss, a' divise q donc $(a \wedge b)a'b'$ divise c. Ceci montre que $(a \wedge b)|a'b'|$ est le ppcm de a et b, que $(a \wedge b)(a \vee b) = (a \wedge b)^2|a'b'| = |ab|$, et que tout multiple commun c de a et b est multiple de $a \vee b$.

4) se déduit alors par calcul direct depuis 2). □

$*$ Ainsi les multiples communs à 4 et 6 sont les multiples de 12.

$*$ Noter que $a \vee b$ est la borne supérieure dans $\mathbb{N}$ muni de la relation d'ordre $|$ de l'ensemble $\{|a|;|b|\}$ (même si a ou b nul), c'est-à-dire le plus élément de l'ensemble formé des majorants communs à a et b.

Autre réponse pour la Pratique 8 : $12 \vee 3 = 12$, $(-10) \vee 15 = 10 \vee 15 = \frac{150}{5} = 30$, et $6 \vee (-5) = 6 \vee 5 = 30$ puisque 6 et 5 sont premiers entre eux.

18►

Preuve : par récurrence sur le nombre n d'entiers a_i. Quitte à renuméroter, on peut supposer $a_0 \neq 0$.
Pour $n = 2$, c'est la relation de Bezout classique.
Supposons $n \geqslant 3$ et supposons le résultat établi pour $n-1$ entiers dont le premier non nul. Il existe donc des entiers u_i' tels que $\sum_{i=1}^{n-1} a_i u_i' = pgcd(a_1, \ldots, a_{n-1})$.
Comme $pgcd(a_1, \ldots, a_n) = pgcd(pgcd(a_1, \ldots, a_{n-1}), a_n)$, il existe α et β entiers
tels que $\alpha pgcd(a_1, \ldots, a_{n-1}) + \beta a_n = pgcd(a_1, \ldots, a_n) = \sum_{i=1}^{n-1} a_i(\alpha u_i') + a_n\beta$, d'où le résultat.
On conclut par le principe de récurrence. □

Pratique 9 :

4, 9 et 10 sont premiers entre eux dans leur ensemble donc de pgcd 1 puisque seuls 1 et -1 divisent tous les trois entiers.
Mais ils ne sont pas premiers entre eux deux à deux puisque 2 divise 4 et 10.

Pratique 10 :

$pgcd(4, 9, 10) = 1$ et $ppcm(4, 9, 10) = 180$, et $4 \times 9 \times 10 = 360$.
Ce serait donc bien d'avoir un outil simple de calcul du pgcd et du ppcm de plus de trois entiers...

Pratique 11 :

On peut utiliser le crible d'Ératosthène, voir plus loin...
Réponse : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$.

19►

Preuve : Montrons 1) par récurrence sur l'entier n considéré. 2 est premier et s'écrit : $2 = 2$
Soit $n \geqslant 3$, et supposons le résultat établi pour tous les entiers $2 \leqslant p \leqslant n-1$.

Si n est premier, c'est fini : $n = n$! Sinon, c'est que n admet un diviseur et s'écrit $n = p \times q$ avec $2 \leqslant p \leqslant n-1$, donc $2 \leqslant q \leqslant n-1$. On utilise l'hypothèse de récurrence qui permet d'écrire p et q comme produits de nombres premiers, ce qui montre que c'est aussi le cas de n. On conclut par le principe de récurrence.

Supposons $\mathbb{P}$ fini, il existerait un plus grand nombre premier N. Considérons le produit des nombres premiers jusqu'à lui, et ajoutons 1, notons n le résultat. Aucun nombre premier inférieur à N ne peut diviser n puisqu'il divise le produit construit mais pas 1. Or 1) nous donne l'existence d'un diviseur premier p pour n, qui ne peut qu'être strictement supérieur à N. Contradiction. □

20►

Principe du crible : on écrit la liste des naturels de 2 à n de gauche à droite, on parcourt ce tableau de gauche à droite.
Si la case rencontrée n'est pas barrée, elle contient un nombre premier, et on barre vers la droite tous ses multiples. Puis on reprend le parcours là où on en était, en passant à la case suivante.
Si la case rencontrée est barrée, elle ne contient pas un nombre premier, et on passe à la case suivante.
n est premier si sa case n'est pas barrée quand on y arrive.

En fait, on peut arrêter le parcours à la case contenant $\lfloor\sqrt{n}\rfloor$ (et la tester). En effet, n est premier si, et seulement si, il n'admet pas de diviseur inférieur ou égal à $\lfloor\sqrt{n}\rfloor$ puisque dans l'écriture $n = pq$, l'un au moins des entiers p et q est inférieur à $\sqrt{n}$.

21►

Preuve : 1) Si p est premier et a entier, les seuls diviseurs de p étant 1 et p, $a \wedge p = p$ si p divise a, et sinon $a \wedge p = 1$.

2) Supposons que p divise ab et p ne divise pas a : d'après 1), a est premier avec a donc divise b d'après le théorème de Gauss, d'où le résultat.

3) On utilise 1) et le fait que p ne divise pas q puisque q est premier, et de même q ne divise pas p. □

22►

∗ *Preuve* : Si $p = 2$ et a entier relatif, $a^2 - a = a(a-1)$ est pair (a ou $a-1$ l'est), c'est-à-dire congru à 0 modulo 2.
Sinon, comme p premier est impair, $(-1)^p = -1$, donc il suffit de montrer le théorème pour a naturel. Par récurrence sur a.
Pour $a = 0$, le résultat est clair.
Soit a un naturel, et supposons $a^p \equiv a\ [p]$.

On calcule : $(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k$ donc $(a+1)^p \equiv a + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k\ [p]$ par hypothèse de récurrence.

Reste à vérifier que les coefficients binomiaux $\binom{p}{k}$, pour $1 \leqslant k \leqslant p-1$, sont multiples de p.

Par la formule efficace, pour un tel coefficient : $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$, donc k divise $p\binom{p-1}{k-1}$. Mais p étant premier et $k < p$, k divise l'entier $\binom{p-1}{k-1}$, donc $\binom{p}{k}$ est bien multiple de p pour $1 \leqslant k \leqslant p-1$. Donc $(a+1)^p \equiv a+1\ [p]$, et on conclut par le principe de récurrence.

Si de plus a n'est pas premier avec p, on a vu qu'il est inversible modulo p ; en multipliant la congruence établie par cet inverse, on obtient $a^{p-1} \equiv 1\ [p]$. □

∗ Par exemple, montrons que tout diviseur premier p de n^2+1 autre que 2 est congru à 1 modulo 4.
On a par hypothèse : $n^2 \equiv -1\ [p]$. Donc n est inversible modulo p (d'inverse $-n$). D'après le petit théorème de Fermat, $n^{p-1} \equiv 1\ [p]$ ou encore $(n^2)^{(p-1)/2} \equiv 1\ [p]$, ce qu'on peut bien écrire puisque p est impair. Donc $(-1)^{(p-1)/2} \equiv 1\ [p]$, et comme p est impair, 1 est différent de -1 modulo p, donc $(p-1)/2$ est pair, d'où le résultat.

23►

∗ *Preuve* : L'existence d'une telle décomposition a déjà été montrée au point 19. Reste l'unicité.

Supposons qu'un naturel $\geqslant 2$ admette deux telles décompositions d_1 et d_2, distinctes. Il existe donc un nombre premier p intervenant dans une des deux décompositions avec une puissance strictement

plus grande que dans l'autre. Après simplification (éventuelle) par la puissance de p la plus petite, on obtient p premier qui divise un produit de puissances de nombres premiers, mais n'y figure pas. Par le théorème de Gauss, p étant premier successivement avec chacun de ses facteurs, on arrive à la contradiction suivante : p divise 1. D'où l'unicité.

Clairement, $p^{\nu_p(n)}$ divise n. Si p^q divise n avec $q > \nu_p(n)$, alors après simplification par $p^{\nu_p(n)}$, on obtient que p divise un produit de puissances de premiers distincts de p, ce qui est impossible comme on vient de le voir. □

$*$ Voilà un outil très pratique, qui simplifie les résolutions de problèmes précédents, comme la recherche pratique d'un pgcd ou d'un ppcm, comme on va le voir plus loin.
Souvenez-vous aussi de la preuve vue en début d'année pour montrer que $\sqrt{2}$ n'est pas un rationnel.

Pratique 12 :

$16 = 2 \times 8 = 2 \times 2 \times 4 = 2^4$, $18 = 2 \times 9 = 2 \times 3^2$, $38 = 2 \times 19$.
Par exemple, les valuations p-adiques de 18 sont toutes nulles sauf $\nu_2(18) = 1$ et $\nu_3(18) = 2$.

24►

Preuve : On effectue le produit des factorisations premières de a et de b : on "range" le résultat sous forme de produit de puissances de nombres premiers, ce qui, par unicité, donne la factorisation première de ab, et dans laquelle on lit les valuations p-adiques.

25►

Preuve : 1) Supposons que a divise b : il existe k entier tel que $b = ak$. Comme conséquence des factorisations premières de a et b, on obtient : $p^{\nu_p(b)}b' = p^{\nu_p(a)}a'k$ avec p premier avec a' et b'. Par unicité de la décomposition première, on obtient $\nu_p(b) = \nu_p(a) + \nu_p(k)$, d'où le résultat.

Réciproquement, si pour tout p premier on a $\nu_p(a) \leqslant \nu_p(b)$, alors on "lit" a dans la factorisation première de b, et a divise b, le quotient étant $\prod_{p\in\mathbb{P}} p^{\nu_p(b)-\nu_p(a)}$.

2) La formule F proposée pour $a \wedge b$ est bien un diviseur de a et de b d'après 1). Inversement, pour tout p premier et c un diviseur de a et de b, on doit avoir d'après a : $\nu_p(c) \leqslant \nu_p(a)$ et $\nu_p(c) \leqslant \nu_p(b)$, donc $\nu_p(c) \leqslant \nu_p(F)$, ce qui montre à nouveau avec 1) que c divise F. Finalement $F = a \wedge b$.
Enfin, comme $|ab| = (a \wedge b) \times (a \vee b)$, on obtient bien la formule de $a \vee b$. □

Pratique 13 :

$432 = 2 \times 216 = 2^2 \times 108 = 2^3 \times 54 = 2^4 \times 27 = 2^4 \times 3^3$, et $328 = 2 \times 164 = 2^2 \times 82 = 2^3 \times 41$.
Donc $432 \wedge 328 = 8$ et $432 \vee 328 = 2^4 \times 3^3 \times 41 = 17712$

26►

Par exemple, si a est premier avec b et avec c, alors a est premier avec bc : aucun facteur premier intervenant "réellement" dans la factorisation première de a n'intervient dans b ni dans c, donc n'intervient pas non plus dans la factorisation première de bc.