CORRIGÉ – CHAPITRE 7

PGCD

PGCD et algorithme d'Euclide

EXERCICE 1 ⋆

1. On décompose chaque nombre pour lire les facteurs communs.
   a) $12 = 2^2 \times 3$ et $42 = 2 \times 3 \times 7$, d'où : $\boxed{\text{PGCD}(12, 42) = 2 \times 3 = 6}$
   b) $45 = 3^2 \times 5$ et $105 = 3 \times 5 \times 7$, d'où : $\boxed{\text{PGCD}(45, 105) = 3 \times 5 = 15}$
   c) $92 = 2^2 \times 23$ et $69 = 3 \times 23$, d'où : $\boxed{\text{PGCD}(92, 69) = 23}$
   d) $72 = 2^3 \times 3^2$ et $108 = 2^2 \times 3^3$, d'où : $\boxed{\text{PGCD}(72, 108) = 2^2 \times 3^2 = 36}$
2. La méthode est la même dans les trois cas. Si $\text{PGCD}(n, N) = d$, alors d divise n, donc $n = d\,n'$; et l'on doit avoir $\text{PGCD}(n', N/d) = 1$.
   a) $\text{PGCD}(n, 324) = 12$ exige d'abord que 12 divise 324, ce qui est vrai ($324 = 12 \times 27$). On pose $n = 12n'$, la condition devient $\text{PGCD}(n', 27) = 1$, c'est-à-dire n' non divisible par 3. Avec $n \leqslant 200$, on a $n' \leqslant 16$:
   $$n' \in \{1\,;2\,;4\,;5\,;7\,;8\,;10\,;11\,;13\,;14\,;16\}$$
   $$\boxed{n \in \{12\,;24\,;48\,;60\,;84\,;96\,;120\,;132\,;156\,;168\,;192\}}$$
   b) $378 = 54 \times 7$. On pose $n = 54n'$ avec $\text{PGCD}(n', 7) = 1$, donc n' non multiple de 7. Avec $n \leqslant 500$, on a $n' \leqslant 9$:
   $$n' \in \{1\,;2\,;3\,;4\,;5\,;6\,;8\,;9\}$$
   $$\boxed{n \in \{54\,;108\,;162\,;216\,;270\,;324\,;432\,;486\}}$$
   On notera que $n' = 7$ est exclu : il donnerait $n = 378$, dont le PGCD avec 378 vaut 378 et non 54.
   c) $150 = 6 \times 25$. On pose $n = 6n'$ avec $\text{PGCD}(n', 25) = 1$, donc n' non multiple de 5. Avec $n \leqslant 400$, on a $n' \leqslant 66$:
   $$\boxed{n = 6n' \text{ où } n' \leqslant 66 \text{ n'est pas un multiple de } 5}$$
   Cela fournit $66 - 13 = 53$ valeurs, les premières étant 6, 12, 18, 24, 36, 42, 48, 54, 66, … et la dernière 396.

EXERCICE 2 ⋆

Méthode commune : si $\text{PGCD}(a, b) = d$, on écrit $a = da'$ et $b = db'$ avec $\text{PGCD}(a', b') = 1$, puis on traduit la seconde condition sur a' et b'.

1. On pose $a = 6a'$ et $b = 6b'$ avec $\text{PGCD}(a', b') = 1$. Alors :
   $$ab = 36a'b' = 432 \qquad \text{d'où} \qquad a'b' = 12$$
   Les couples (a', b') avec $a' < b'$, de produit 12 et premiers entre eux, sont $(1\,;12)$ et $(3\,;4)$ — le couple $(2\,;6)$ est à écarter car $\text{PGCD}(2, 6) = 2$.
   $$\boxed{(a\,;b) \in \{(6\,;72)\,;\,(18\,;24)\}}$$
   Vérification : $6 \times 72 = 432$ et $\text{PGCD}(6, 72) = 6$; $18 \times 24 = 432$ et $\text{PGCD}(18, 24) = 6$.

2. On pose $a = 18a'$ et $b = 18b'$, d'où $324a'b' = 7776$, soit $a'b' = 24$. Les couples premiers entre eux avec $a' < b'$ sont $(1\,;24)$ et $(3\,;8)$.

$$\boxed{(a\,;b) \in \{(18\,;432)\,;\,(54\,;144)\}}$$

3. On pose $a = 4a'$ et $b = 4b'$, d'où $4(a' + b') = 24$, soit $a' + b' = 6$. Les couples premiers entre eux avec $a' < b'$ sont : $(1\,;5)$ seulement, car $(2\,;4)$ a pour PGCD 2 et $(3\,;3)$ ne vérifie pas $a' < b'$.

$$\boxed{(a\,;b) = (4\,;20)}$$

EXERCICE 3 ⋆

1. On applique l'algorithme d'Euclide : le PGCD est le *dernier reste non nul*.

a)

$$\begin{aligned} 840 &= 144 \times 5 + 120 \\ 144 &= 120 \times 1 + 24 \\ 120 &= 24 \times 5 + 0 \end{aligned}$$

$$\boxed{\text{PGCD}(144, 840) = 24}$$

b)

$$\begin{aligned} 202 &= 138 \times 1 + 64 \\ 138 &= 64 \times 2 + 10 \\ 64 &= 10 \times 6 + 4 \\ 10 &= 4 \times 2 + 2 \\ 4 &= 2 \times 2 + 0 \end{aligned}$$

$$\boxed{\text{PGCD}(202, 138) = 2}$$

c)

$$\begin{aligned} 777 &= 441 \times 1 + 336 \\ 441 &= 336 \times 1 + 105 \\ 336 &= 105 \times 3 + 21 \\ 105 &= 21 \times 5 + 0 \end{aligned}$$

$$\boxed{\text{PGCD}(441, 777) = 21}$$

d)

$$\begin{aligned} 9185 &= 2004 \times 4 + 1169 \\ 2004 &= 1169 \times 1 + 835 \\ 1169 &= 835 \times 1 + 334 \\ 835 &= 334 \times 2 + 167 \\ 334 &= 167 \times 2 + 0 \end{aligned}$$

$$\boxed{\text{PGCD}(2004, 9185) = 167}$$

2. a)

$$5633 = 4847 \times 1 + 786$$
$$4847 = 786 \times 6 + 131$$
$$786 = 131 \times 6 + 0$$

$$\text{PGCD}(4847, 5633) = 131 \neq 1$$

$$\boxed{\text{4847 et 5633 ne sont pas premiers entre eux}}$$

b)

$$5617 = 813 \times 6 + 739$$
$$813 = 739 \times 1 + 74$$
$$739 = 74 \times 9 + 73$$
$$74 = 73 \times 1 + 1$$
$$73 = 1 \times 73 + 0$$

$$\text{PGCD}(5617, 813) = 1$$

$$\boxed{\text{5617 et 813 sont premiers entre eux}}$$

EXERCICE 4 ⋆

1. On applique l'algorithme d'Euclide, puis on divise numérateur et dénominateur par le PGCD.

$$3780 = 3528 \times 1 + 252 \quad ; \quad 3528 = 252 \times 14 + 0$$

Donc $\text{PGCD}(3528, 3780) = 252$, et :

$$\boxed{\frac{3528}{3780} = \frac{252 \times 14}{252 \times 15} = \frac{14}{15}}$$

$$1071 = 462 \times 2 + 147 \quad ; \quad 462 = 147 \times 3 + 21 \quad ; \quad 147 = 21 \times 7 + 0$$

Donc $\text{PGCD}(1071, 462) = 21$, et :

$$\boxed{\frac{1071}{462} = \frac{21 \times 51}{21 \times 22} = \frac{51}{22}}$$

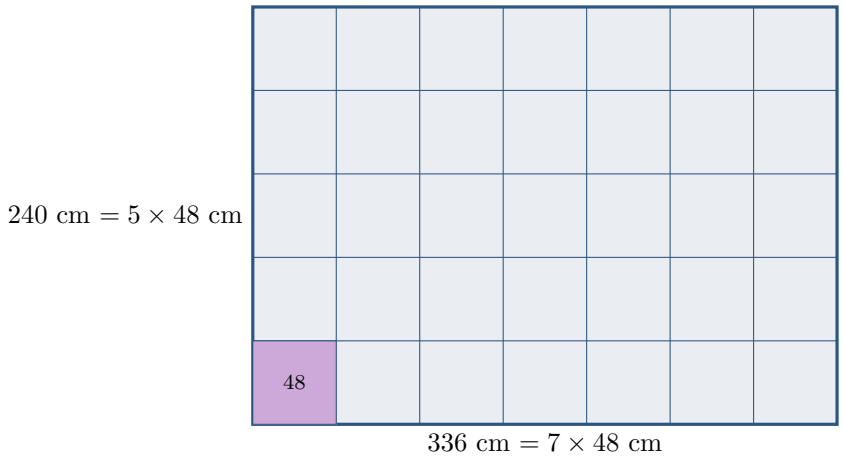
Une fraction divisée par le PGCD de ses deux termes est irréductible : si $a = da'$ et $b = db'$ avec $d = \text{PGCD}(a, b)$, la Proposition 3 donne $d = d \times \text{PGCD}(a', b')$, donc $\text{PGCD}(a', b') = 1$.

2. On travaille en centimètres : 336 cm sur 240 cm. Le côté c d'une dalle doit diviser à la fois 336 et 240 pour qu'il n'y ait pas de découpe, et l'on veut c le plus grand possible : $c = \text{PGCD}(336, 240)$.

$$336 = 240 \times 1 + 96 \quad ; \quad 240 = 96 \times 2 + 48 \quad ; \quad 96 = 48 \times 2 + 0$$

$$\boxed{c = 48 \text{ cm}}$$

Il y a $\frac{336}{48} = 7$ dalles dans la longueur et $\frac{240}{48} = 5$ dans la largeur, soit $\boxed{7 \times 5 = 35 \text{ dalles}}$.



La pièce est découpée en 7×5 carrés de 48 cm de côté ; la dalle violette en donne un exemple. Une dalle plus grande ne pourrait pas mesurer exactement à la fois 336 et 240 cm en un nombre entier d'exemplaires, puisque 48 est le plus grand diviseur commun de ces deux longueurs.

EXERCICE 5 ⋆⋆

Notons d l'entier cherché. Les divisions euclidiennes s'écrivent :

$$4294 = dq + 10 \qquad \text{et} \qquad 3521 = dq' + 11$$

où q et q' sont des entiers. On en déduit :

$$4294 - 10 = 4284 = dq \qquad \text{et} \qquad 3521 - 11 = 3510 = dq'$$

Autrement dit, d est un **diviseur commun** à 4284 et 3510, donc un diviseur de leur PGCD. Calculons-le par l'algorithme d'Euclide :

$$\begin{aligned} 4284 &= 3510 \times 1 + 774 \\ 3510 &= 774 \times 4 + 414 \\ 774 &= 414 \times 1 + 360 \\ 414 &= 360 \times 1 + 54 \\ 360 &= 54 \times 6 + 36 \\ 54 &= 36 \times 1 + 18 \\ 36 &= 18 \times 2 + 0 \end{aligned}$$

$$\text{PGCD}(4284, 3510) = 18$$

Les valeurs possibles de d sont donc les diviseurs de 18, à savoir 1, 2, 3, 6, 9 et 18. Mais un reste est toujours *strictement inférieur* au diviseur : comme le reste 11 apparaît, il faut $d > 11$.

$$\boxed{d = 18}$$

Vérification : $4294 = 18 \times 238 + 10$ et $3521 = 18 \times 195 + 11$.

EXERCICE 6 ⋆⋆

1. d divise n et $n+6$, donc leur différence $(n+6)-n=6$. Les valeurs possibles sont les diviseurs positifs de 6 :

$$\boxed{d \in \{1\,;2\,;3\,;6\}}$$

2. Réciproquement, un diviseur commun à n et 6 divise $n+6$. Les diviseurs communs de n et $n+6$ sont donc exactement ceux de n et 6, d'où $d = \text{PGCD}(n,6)$. Si $n = 6q+r$ avec $0 \leqslant r \leqslant 5$, la Proposition 2 donne $d = \text{PGCD}(6,r)$ lorsque $r \neq 0$, et $d = 6$ lorsque $r = 0$:

Reste de n modulo 6	0	1	2	3	4	5
$d = \text{PGCD}(n, n+6)$	6	1	2	3	2	1

3. $n = 9$ a pour reste 3 : $\text{PGCD}(9,15) = 3$. $n = 10$ a pour reste 4 : $\text{PGCD}(10,16) = 2$. $n = 11$ a pour reste 5 : $\text{PGCD}(11,17) = 1$. $n = 12$ a pour reste 0 : $\text{PGCD}(12,18) = 6$. Les quatre valeurs sont conformes au tableau.

EXERCICE 7 ⋆⋆

1. Si δ divise a et b, il divise la combinaison linéaire $b-ka$. Réciproquement, si δ divise a et $b-ka$, il divise $(b-ka)+ka = b$. Les couples $(a\,;b)$ et $(a\,;b-ka)$ ont donc les mêmes diviseurs communs, et en particulier le même plus grand :

$$\boxed{\text{PGCD}(a,b) = \text{PGCD}(a, b-ka)}$$

La Proposition 2 du cours est le cas particulier où k est le quotient de la division euclidienne de b par a.

2. Avec $a = n+2$, $b = 3n+5$ et $k = 3$: $b-3a = 3n+5-3n-6 = -1$. D'après la Proposition 1 :

$$\text{PGCD}(3n+5, n+2) = \text{PGCD}(n+2, -1) = \text{PGCD}(n+2, 1) = \boxed{1}$$

3. On développe : $(n-1)(n+1)+4 = n^2-1+4 = n^2+3$. Avec $a = n+1$, $b = n^2+3$ et $k = n-1$:

$$\text{PGCD}(n^2+3, n+1) = \text{PGCD}(n+1, 4)$$

qui est un diviseur de 4. On discute selon le reste de n modulo 4 :

- si n est pair, $n+1$ est impair : $\text{PGCD}(n+1,4) = 1$;
- si $n \equiv 1\ [4]$, $n+1 \equiv 2\ [4]$: $n+1$ est pair mais non multiple de 4, donc $\text{PGCD}(n+1,4) = 2$;
- si $n \equiv 3\ [4]$, $n+1 \equiv 0\ [4]$: $\text{PGCD}(n+1,4) = 4$.

$$\boxed{\text{PGCD}(n^2+3, n+1) = \begin{cases} 1 & \text{si } n \text{ est pair} \\ 2 & \text{si } n \equiv 1\ [4] \\ 4 & \text{si } n \equiv 3\ [4] \end{cases}}$$

Contrôle : pour $n = 3$, $\text{PGCD}(12,4) = 4$; pour $n = 5$, $\text{PGCD}(28,6) = 2$; pour $n = 4$, $\text{PGCD}(19,5) = 1$.

EXERCICE 8 ⋆⋆

1. Le nombre D divise a et b, donc toute combinaison linéaire de a et b. Cherchons une combinaison qui élimine n :

$$2a-5b = 2(5n+1)-5(2n-1) = 10n+2-10n+5 = 7$$

Ainsi D divise 7. Or 7 est premier, ses seuls diviseurs positifs sont 1 et 7.

$$\boxed{D = 1 \quad \text{ou} \quad D = 7}$$

2. On résout les deux congruences séparément.
   $a \equiv 0\ [7]$ signifie $5n+1 \equiv 0\ [7]$, soit $5n \equiv -1 \equiv 6\ [7]$. En multipliant par 3, qui est l'inverse de 5 modulo 7 puisque $5 \times 3 = 15 \equiv 1\ [7]$:

$$n \equiv 18 \equiv 4\ [7]$$

   $b \equiv 0\ [7]$ signifie $2n-1 \equiv 0\ [7]$, soit $2n \equiv 1\ [7]$. Comme $2 \times 4 = 8 \equiv 1\ [7]$, l'inverse de 2 est 4 :

$$n \equiv 4\ [7]$$

   Les deux conditions coïncident :

$$\boxed{a \equiv 0\ [7] \text{ et } b \equiv 0\ [7] \iff n \equiv 4\ [7]}$$

3. Si $n \equiv 4\ [7]$, alors 7 divise à la fois a et b, donc 7 divise D ; comme $D \in \{1\,;7\}$, on a $D = 7$. Sinon, 7 ne divise pas a, donc $D \neq 7$, et $D = 1$.

$$\boxed{D = \begin{cases} 7 & \text{si } n \equiv 4\ [7] \\ 1 & \text{sinon} \end{cases}}$$

   Vérification pour $n = 4$: $a = 21$ et $b = 7$, de PGCD 7. Pour $n = 5$: $a = 26$ et $b = 9$, de PGCD 1.

EXERCICE 9 ⋆

Dans les trois questions, on utilise le **théorème de Bézout** : deux entiers sont premiers entre eux si et seulement s'il existe une combinaison linéaire d'entre eux égale à 1.

1. On cherche à éliminer n entre $a = 7n+4$ et $b = 5n+3$:

$$5a - 7b = 5(7n+4) - 7(5n+3) = 35n + 20 - 35n - 21 = -1$$

   d'où, en changeant les signes :

$$(-5) \times a + 7 \times b = 1$$

   Le couple $(-5\,;7)$ convient. D'après le théorème de Bézout :

$$\boxed{\text{Pour tout } n \in \mathbb{N},\ a \text{ et } b \text{ sont premiers entre eux}}$$

2. Soient n et $n+1$ deux entiers consécutifs non nuls. Alors :

$$1 \times (n+1) + (-1) \times n = 1$$

$$\boxed{\text{Deux entiers consécutifs sont toujours premiers entre eux}}$$

3. Soient $2n+1$ et $2n+3$ deux entiers impairs consécutifs, et d leur PGCD. Alors d divise leur différence :

$$(2n+3) - (2n+1) = 2$$

   donc d divise 2, c'est-à-dire $d = 1$ ou $d = 2$. Mais d divise $2n+1$, qui est impair : d ne peut donc pas valoir 2.

$$\boxed{\text{Deux entiers impairs consécutifs sont premiers entre eux}}$$

EXERCICE 10 ⋆

Une fraction $\frac{p}{q}$ est irréductible si et seulement si $\text{PGCD}(p,q) = 1$. On exhibe donc à chaque fois une combinaison linéaire égale à 1 (théorème de Bézout).

a)

$$(-2) \times n + 1 \times (2n+1) = -2n + 2n + 1 = 1$$

$$\boxed{\text{PGCD}(n, 2n+1) = 1 : \text{la fraction est irréductible}}$$

b)

$$2 \times (9n+1) - 3 \times (6n+1) = 18n + 2 - 18n - 3 = -1$$

d'où $(-2)(9n+1) + 3(6n+1) = 1$:

$$\boxed{\text{PGCD}(9n+1, 6n+1) = 1 : \text{la fraction est irréductible}}$$

c)

$$5 \times (14n+3) - 14 \times (5n+1) = 70n + 15 - 70n - 14 = 1$$

$$\boxed{\text{PGCD}(14n+3, 5n+1) = 1 : \text{la fraction est irréductible}}$$

Le procédé est toujours le même : on multiplie les deux expressions par les coefficients croisés de n, de façon à faire disparaître n dans la différence.

EXERCICE 11 ⋆⋆

1. On factorise les deux expressions. Pour a :

$$a = n^3 - n^2 - 12n = n\left(n^2 - n - 12\right) = n(n-4)(n+3)$$

car $n^2 - n - 12$ a pour racines 4 et -3. Pour b :

$$b = 2n^2 - 7n - 4 = (n-4)(2n+1)$$

ce que l'on vérifie en développant : $(n-4)(2n+1) = 2n^2 + n - 8n - 4 = 2n^2 - 7n - 4$.

$$\boxed{a = n(n-4)(n+3) \qquad ; \qquad b = (n-4)(2n+1)}$$

Comme $n > 5$, les trois facteurs n, $n-4$ et $n+3$ sont des entiers strictement positifs, de même que $2n+1$:

$$\boxed{a \text{ et } b \text{ sont des entiers naturels divisibles par } n-4}$$

2. (a) d divise $\alpha = 2n+1$ et $\beta = n+3$, donc toute combinaison linéaire :

$$2\beta - \alpha = 2(n+3) - (2n+1) = 2n + 6 - 2n - 1 = 5$$

$$\boxed{d \text{ divise } 5, \text{ donc } d = 1 \text{ ou } d = 5}$$

(b) Traitons la double implication. D'une part :

$$\beta \equiv 0\ [5] \iff n+3 \equiv 0\ [5] \iff n \equiv -3 \equiv 2\ [5] \iff n-2 \equiv 0\ [5]$$

D'autre part, si $n \equiv 2\ [5]$, alors :

$$\alpha = 2n+1 \equiv 2 \times 2 + 1 = 5 \equiv 0\ [5]$$

Réciproquement, si $\alpha \equiv 0\ [5]$, alors $2n \equiv -1 \equiv 4\ [5]$, donc $n \equiv 2\ [5]$ en multipliant par 3, inverse de 2 modulo 5.

$$\boxed{\alpha \text{ et } \beta \text{ sont multiples de } 5 \iff n-2 \equiv 0\ [5]}$$

3.
$$1 \times (2n+1) - 2 \times n = 1$$
D'après le théorème de Bézout :
$$\boxed{2n+1 \text{ et } n \text{ sont premiers entre eux}}$$

4. (a) Les deux nombres s'écrivent $a = (n-4) \times n(n+3)$ et $b = (n-4) \times (2n+1)$, donc :
$$\text{PGCD}(a,b) = (n-4) \times \text{PGCD}(n(n+3)\,,\,2n+1)$$
Soit δ un diviseur commun positif de $n(n+3)$ et $2n+1$. Un diviseur commun de δ et de n divise $2n+1$ et n, donc 1 d'après la question 3 : δ est premier avec n. Comme δ divise $n(n+3)$, le théorème de Gauss donne $\delta \mid n+3$. Réciproquement, un diviseur commun de $n+3$ et $2n+1$ divise $n(n+3)$. Les deux couples ont donc les mêmes diviseurs communs :
$$\text{PGCD}(n(n+3)\,,\,2n+1) = \text{PGCD}(n+3\,,\,2n+1) = d$$
D'après les questions 2a et 2b, d vaut 5 lorsque $n \equiv 2\ [5]$, et 1 sinon.
$$\boxed{\text{PGCD}(a,b) = \begin{cases} 5(n-4) & \text{si } n \equiv 2\ [5] \\ n-4 & \text{sinon} \end{cases}}$$

(b) Pour $n = 11$: on a $11 = 5 \times 2 + 1$, donc $n \not\equiv 2\ [5]$ et le PGCD vaut $n - 4 = 7$. On vérifie :
$$a = 11 \times 7 \times 14 = 1078 \quad ; \quad b = 7 \times 23 = 161$$
et $\text{PGCD}(1078, 161) = 7$. Cohérent

Pour $n = 12$: on a $12 = 5 \times 2 + 2$, donc $n \equiv 2\ [5]$ et le PGCD vaut $5(n-4) = 40$. On vérifie :
$$a = 12 \times 8 \times 15 = 1440 \quad ; \quad b = 8 \times 25 = 200$$
et $\text{PGCD}(1440, 200) = 40$. Cohérent

Théorème de Bézout et algorithme d'Euclide étendu

EXERCICE 12 ⋆

1. Étape 1 : l'algorithme d'Euclide.
$$\begin{aligned} 87 &= 31 \times 2 + 25 \quad (L_1) \\ 31 &= 25 \times 1 + 6 \quad (L_2) \\ 25 &= 6 \times 4 + 1 \quad (L_3) \\ 6 &= 1 \times 6 + 0 \end{aligned}$$
Le dernier reste non nul vaut 1, donc $\text{PGCD}(87, 31) = 1$: 87 et 31 sont premiers entre eux

Étape 2 : la remontée. On isole le 1 dans (L_3), puis on remplace successivement les restes en remontant les lignes, de façon à faire réapparaître 87 et 31.
$$\begin{aligned} 1 &= 25 - 6 \times 4 && \text{or d'après } (L_2),\ 6 = 31 - 25 \times 1 \\ &= 25 - (31 - 25) \times 4 \\ &= 25 - 31 \times 4 + 25 \times 4 \\ &= 5 \times 25 - 31 \times 4 && \text{or d'après } (L_1),\ 25 = 87 - 31 \times 2 \\ &= 5 \times (87 - 31 \times 2) - 31 \times 4 \\ &= 5 \times 87 - 31 \times 10 - 31 \times 4 \\ &= 5 \times 87 - 14 \times 31 \end{aligned}$$

$$\boxed{(x\,;y) = (5\,;-14) \quad \text{car} \quad 87\times 5 + 31\times(-14) = 1}$$

Vérification : $435 - 434 = 1$.

2. Algorithme d'Euclide appliqué à 45 et 38 :

$$\begin{aligned} 45 &= 38\times 1 + 7 \qquad (L_1)\\ 38 &= 7\times 5 + 3 \qquad (L_2)\\ 7 &= 3\times 2 + 1 \qquad (L_3)\\ 3 &= 1\times 3 + 0 \end{aligned}$$

$\text{PGCD}(38,45) = 1$: $\boxed{\text{38 et 45 sont premiers entre eux}}$

Remontée :

$$\begin{aligned} 1 &= 7 - 3\times 2 && \text{or d'après } (L_2),\ 3 = 38 - 7\times 5\\ &= 7 - (38 - 7\times 5)\times 2\\ &= 7 - 38\times 2 + 7\times 10\\ &= 11\times 7 - 38\times 2 && \text{or d'après } (L_1),\ 7 = 45 - 38\times 1\\ &= 11\times(45-38) - 38\times 2\\ &= 11\times 45 - 38\times 11 - 38\times 2\\ &= -13\times 38 + 11\times 45 \end{aligned}$$

$$\boxed{(x\,;y) = (-13\,;11) \quad \text{car} \quad 38\times(-13) + 45\times 11 = 1}$$

Vérification : $-494 + 495 = 1$.

3. Algorithme d'Euclide appliqué à 41 et 25 :

$$\begin{aligned} 41 &= 25\times 1 + 16 \qquad (L_1)\\ 25 &= 16\times 1 + 9 \qquad (L_2)\\ 16 &= 9\times 1 + 7 \qquad (L_3)\\ 9 &= 7\times 1 + 2 \qquad (L_4)\\ 7 &= 2\times 3 + 1 \qquad (L_5)\\ 2 &= 1\times 2 + 0 \end{aligned}$$

$\text{PGCD}(41,25) = 1$: $\boxed{\text{41 et 25 sont premiers entre eux}}$

Remontée : elle comporte ici quatre substitutions.

$$\begin{aligned} 1 &= 7 - 2\times 3 && \text{or } (L_4) :\ 2 = 9 - 7\\ &= 7 - (9-7)\times 3 = 4\times 7 - 3\times 9 && \text{or } (L_3) :\ 7 = 16 - 9\\ &= 4\times(16-9) - 3\times 9 = 4\times 16 - 7\times 9 && \text{or } (L_2) :\ 9 = 25 - 16\\ &= 4\times 16 - 7\times(25-16) = 11\times 16 - 7\times 25 && \text{or } (L_1) :\ 16 = 41 - 25\\ &= 11\times(41-25) - 7\times 25 = 11\times 41 - 18\times 25 \end{aligned}$$

L'équation demandée étant $41x - 25y = 1$, on identifie directement :

$$\boxed{(x\,;y) = (11\,;18) \quad \text{car} \quad 41\times 11 - 25\times 18 = 1}$$

Vérification : $451 - 450 = 1$.

4. Algorithme d'Euclide appliqué à 331 et 221 :

$$\begin{aligned} 331 &= 221 \times 1 + 110 \qquad (L_1) \\ 221 &= 110 \times 2 + 1 \qquad (L_2) \\ 110 &= 1 \times 110 + 0 \end{aligned}$$

$\text{PGCD}(221, 331) = 1$: $\boxed{\text{221 et 331 sont premiers entre eux}}$

Remontée : elle est très courte, une seule substitution suffit.

$$\begin{aligned} 1 &= 221 - 110 \times 2 \qquad \text{or d'après } (L_1),\ 110 = 331 - 221 \\ &= 221 - (331 - 221) \times 2 \\ &= 221 + 221 \times 2 - 331 \times 2 \\ &= 3 \times 221 - 2 \times 331 \end{aligned}$$

L'équation demandée étant $221x - 331y = 1$:

$$\boxed{(x\,;y) = (3\,;2) \quad \text{car} \quad 221 \times 3 - 331 \times 2 = 1}$$

Vérification : $663 - 662 = 1$.

EXERCICE 13 : INVERSE MODULAIRE ET CHIFFREMENT AFFINE ⋆⋆

1. Algorithme d'Euclide :

$$\begin{aligned} 26 &= 11 \times 2 + 4 \qquad (L_1) \\ 11 &= 4 \times 2 + 3 \qquad (L_2) \\ 4 &= 3 \times 1 + 1 \qquad (L_3) \end{aligned}$$

Remontée :

$$\begin{aligned} 1 &= 4 - 3 \qquad \text{or } (L_2) :\ 3 = 11 - 4 \times 2 \\ &= 4 - (11 - 4 \times 2) = 3 \times 4 - 11 \qquad \text{or } (L_1) :\ 4 = 26 - 11 \times 2 \\ &= 3 \times (26 - 11 \times 2) - 11 = 3 \times 26 - 7 \times 11 \end{aligned}$$

$$\boxed{(u\,;v) = (-7\,;3) \quad \text{car} \quad 11 \times (-7) + 26 \times 3 = -77 + 78 = 1}$$

On en déduit $11 \times (-7) \equiv 1\ [26]$. Comme $-7 \equiv 19\ [26]$:

$$\boxed{x_0 = 19} \qquad \text{vérification : } 11 \times 19 = 209 = 8 \times 26 + 1$$

2. Si $11x \equiv 5\ [26]$, on multiplie par 19 : $209x \equiv 95\ [26]$, c'est-à-dire $x \equiv 95 \equiv 17\ [26]$, car $209 \equiv 1$ et $95 = 3 \times 26 + 17$. Réciproquement, si $x \equiv 17\ [26]$, alors $11x \equiv 187 = 7 \times 26 + 5 \equiv 5\ [26]$.

$$\boxed{S = \{17 + 26k\ ;\ k \in \mathbb{Z}\}}$$

Multiplier par l'inverse de 11 joue le même rôle que diviser par 11 dans une équation réelle.

3. (a) E a pour rang 4 : $11 \times 4 + 3 = 47 = 26 + 21$, donc $y = 21$, qui est le rang de V. $\boxed{E \text{ est codé en } V}$

   (b) Si $y \equiv 11x + 3\ [26]$, alors $y - 3 \equiv 11x$, et en multipliant par 19 : $19(y - 3) \equiv 209x \equiv x\ [26]$. Réciproquement, si $x \equiv 19(y - 3)$, alors $11x \equiv 209(y - 3) \equiv y - 3\ [26]$. Pour H, de rang 7 :

$$x \equiv 19 \times 4 = 76 = 2 \times 26 + 24 \equiv 24\ [26]$$

$$\boxed{H \text{ se décode en } Y}$$

On vérifie : $11 \times 24 + 3 = 267 = 10 \times 26 + 7$, qui est bien le rang de H.

(c) 13 et 26 ne sont pas premiers entre eux : 13 n'a pas d'inverse modulo 26. Concrètement, $13x$ est congru à 0 ou à 13 modulo 26 selon la parité de x, donc $13x+3$ ne prend que les valeurs 3 et 16 modulo 26. Par exemple, A et C sont tous deux codés en D : le décodage est impossible.

EXERCICE 14 ⋆

1. L'équation $33x - 45y = 0$ s'écrit $33x = 45y$. Comme $\text{PGCD}(33, 45) = 3$, on simplifie par 3 :

$$11x = 15y$$

Ainsi 11 divise $15y$. Or $\text{PGCD}(11, 15) = 1$, donc d'après le **théorème de Gauss**, 11 divise y : il existe $k \in \mathbb{Z}$ tel que $y = 11k$. En reportant :

$$11x = 15 \times 11k \qquad \text{d'où} \qquad x = 15k$$

$$\boxed{S = \{(15k\,;11k)\ ;\ k \in \mathbb{Z}\}}$$

Vérification : $33 \times 15k - 45 \times 11k = 495k - 495k = 0$.

2. L'équation $33x + 45y = 12$ admet des solutions car $\text{PGCD}(33, 45) = 3$ divise 12. On simplifie d'abord par 3 :

$$11x + 15y = 4$$

Solution particulière : on remarque que $11 \times (-1) + 15 \times 1 = 4$, donc le couple $(-1\,;1)$ convient.

Solutions générales : soit $(x\,;y)$ une solution. On soustrait terme à terme :

$$\begin{cases} 11x + 15y = 4 \\ 11 \times (-1) + 15 \times 1 = 4 \end{cases} \qquad \Longrightarrow \qquad 11(x+1) + 15(y-1) = 0$$

soit $11(x+1) = 15(1-y)$. Comme 11 et 15 sont premiers entre eux et que 11 divise $15(1-y)$, le théorème de Gauss donne $11 \mid (1-y)$: il existe $k \in \mathbb{Z}$ tel que $1-y = 11k$, c'est-à-dire $y = 1-11k$. En reportant, $11(x+1) = 15 \times 11k$, d'où $x = 15k - 1$.

$$\boxed{S = \{(15k-1\,;1-11k)\ ;\ k \in \mathbb{Z}\}}$$

Vérification : $33(15k-1) + 45(1-11k) = 495k - 33 + 45 - 495k = 12$.

EXERCICE 15 ⋆

1. L'équation $7(x-3) = 5(y-2)$ montre que 5 divise $7(x-3)$. Or $\text{PGCD}(5, 7) = 1$, donc d'après le théorème de Gauss, 5 divise $x-3$: il existe $k \in \mathbb{Z}$ tel que :

$$x - 3 = 5k \qquad \text{c'est-à-dire} \qquad x = 5k + 3$$

En reportant dans l'équation : $7 \times 5k = 5(y-2)$, d'où $y - 2 = 7k$ et $y = 7k + 2$.

$$\boxed{S = \{(5k+3\,;7k+2)\ ;\ k \in \mathbb{Z}\}}$$

2. $7x \equiv 1\ [5]$ signifie que 5 divise $7x - 1$, c'est-à-dire qu'il existe un entier y tel que $7x - 1 = 5y$, soit $7x - 5y = 1$. On fait apparaître l'équation précédente en écrivant :

$$7x - 5y = 1 \iff 7x - 21 = 5y - 20 \iff 7(x-3) = 5(y-4)$$

Le raisonnement de la question 1 s'applique à l'identique : $x - 3 = 5k$, donc :

$$\boxed{x \equiv 3\ [5],\ \text{c'est-à-dire } x = 5k + 3 \text{ où } k \in \mathbb{Z}}$$

Vérification : $7 \times 3 = 21 = 4 \times 5 + 1$, donc $7 \times 3 \equiv 1\ [5]$.

Équations diophantiennes

EXERCICE 16 ⋆

1. D'après le corollaire de Bézout, l'équation $ax+by=c$ admet des solutions entières si et seulement si PGCD(a,b) divise c. Ici :
$$\text{PGCD}(4,3)=1$$
et 1 divise 2.
$$\boxed{\text{L'équation admet des solutions entières}}$$

2. On cherche une solution évidente : $4\times 2-3\times 2=8-6=2$.
$$\boxed{(x_0\,;y_0)=(2\,;2)}$$

3. Soit $(x\,;y)$ une solution. On soustrait terme à terme :
$$\begin{cases} 4x-3y=2 \\ 4\times 2-3\times 2=2 \end{cases} \quad\Longrightarrow\quad 4(x-2)-3(y-2)=0$$
soit $4(x-2)=3(y-2)$. Comme 3 divise $4(x-2)$ et que PGCD$(3,4)=1$, le théorème de Gauss donne $3\mid(x-2)$: il existe $k\in\mathbb{Z}$ tel que $x-2=3k$, soit $x=3k+2$. En reportant, $4\times 3k=3(y-2)$, d'où $y=4k+2$.
$$\boxed{S=\{(3k+2\,;4k+2)\ ;\ k\in\mathbb{Z}\}}$$
Vérification : $4(3k+2)-3(4k+2)=12k+8-12k-6=2$.
Cette vérification est indispensable : le raisonnement précédent procède par implication.

EXERCICE 17 ⋆

1. PGCD$(3,4)=1$ divise 6 : l'équation admet des solutions. On en trouve une immédiatement en prenant $y=0$:
$$3\times 2-4\times 0=6 \qquad \text{d'où} \qquad \boxed{(x_0\,;y_0)=(2\,;0)}$$

2. Soit $(x\,;y)$ une solution. En soustrayant terme à terme :
$$3(x-2)-4(y-0)=0 \qquad \text{soit} \qquad 3(x-2)=4y$$
Comme 4 divise $3(x-2)$ et que PGCD$(3,4)=1$, le théorème de Gauss donne $4\mid(x-2)$: il existe $k\in\mathbb{Z}$ tel que $x=4k+2$. En reportant, $3\times 4k=4y$, d'où $y=3k$.
$$\boxed{S=\{(4k+2\,;3k)\ ;\ k\in\mathbb{Z}\}}$$
Vérification : $3(4k+2)-4\times 3k=12k+6-12k=6$.

EXERCICE 18 ⋆

1. PGCD$(5,8)=1$ divise 2 : l'équation admet des solutions. On cherche d'abord une solution de $5x+8y=1$: comme $5\times(-3)+8\times 2=-15+16=1$, le couple $(-3\,;2)$ convient. En multipliant par 2 :
$$5\times(-6)+8\times 4=2 \qquad \text{d'où} \qquad (x_0\,;y_0)=(-6\,;4)$$
On peut aussi remarquer directement que $5\times 2+8\times(-1)=2$:
$$\boxed{(x_0\,;y_0)=(2\,;-1)}$$

2. Soit $(x\,;y)$ une solution. En soustrayant terme à terme :

$$5(x-2)+8(y+1)=0 \qquad \text{soit} \qquad 5(x-2)=-8(y+1)$$

Comme 8 divise $5(x-2)$ et que $\text{PGCD}(5,8)=1$, le théorème de Gauss donne $8 \mid (x-2)$: il existe $k\in\mathbb{Z}$ tel que $x=8k+2$. En reportant, $5\times 8k=-8(y+1)$, d'où $y+1=-5k$ et $y=-5k-1$.

$$\boxed{S=\{(8k+2\,;-5k-1)\ ;\ k\in\mathbb{Z}\}}$$

Vérification : $5(8k+2)+8(-5k-1)=40k+10-40k-8=2$.

EXERCICE 19 ⋆

1. $\text{PGCD}(6,9)=3$. D'après le corollaire de Bézout, $6x+9y=c$ a des solutions entières si et seulement si 3 divise c.

$$\boxed{6x+9y=20 \text{ n'a pas de solution entière, } 6x+9y=21 \text{ en a}}$$

On peut aussi le voir directement : $6x+9y$ est toujours un multiple de 3, ce que 20 n'est pas.

2. On divise par 3 : l'équation équivaut à $2x+3y=7$. Le couple $(2\,;1)$ est solution évidente, car $4+3=7$. Si $(x\,;y)$ est solution, en soustrayant :

$$2(x-2)+3(y-1)=0 \qquad \text{soit} \qquad 2(x-2)=3(1-y)$$

Comme 3 divise $2(x-2)$ et que $\text{PGCD}(2,3)=1$, le théorème de Gauss donne $x-2=3k$ avec $k\in\mathbb{Z}$, puis $y=1-2k$.

$$\boxed{S=\{(2+3k\,;1-2k)\ ;\ k\in\mathbb{Z}\}}$$

Vérification : $6(2+3k)+9(1-2k)=12+18k+9-18k=21$. **L'erreur la plus répandue** est d'oublier de simplifier par 3 : on obtiendrait alors $x=2+9k$, $y=1-6k$, et l'on perdrait les deux tiers des solutions.

EXERCICE 20 ⋆

1. Algorithme d'Euclide appliqué à 23 et 13 :

$$\begin{aligned} 23&=13\times 1+10 \qquad (L_1)\\ 13&=10\times 1+3 \qquad (L_2)\\ 10&=3\times 3+1 \qquad (L_3)\\ 3&=1\times 3+0 \end{aligned}$$

Le dernier reste non nul vaut 1, donc $\text{PGCD}(13,23)=1$ et l'équation admet des solutions.

Remontée :

$$\begin{aligned} 1&=10-3\times 3 && \text{or d'après } (L_2),\ 3=13-10\\ &=10-(13-10)\times 3 &&\\ &=4\times 10-13\times 3 && \text{or d'après } (L_1),\ 10=23-13\\ &=4\times(23-13)-13\times 3 &&\\ &=4\times 23-13\times 4-13\times 3 &&\\ &=4\times 23-7\times 13 && \end{aligned}$$

On obtient $-7\times 13+4\times 23=1$, que l'on réécrit sous la forme demandée $13x-23y=1$:

$$13\times(-7)-23\times(-4)=-91+92=1$$

$$\boxed{(x_0\,;y_0)=(-7\,;-4)}$$

2. Soit $(x\,;y)$ une solution. En soustrayant terme à terme :

$$13(x+7)-23(y+4)=0 \qquad \text{soit} \qquad 13(x+7)=23(y+4)$$

Comme 23 divise $13(x+7)$ et que $\text{PGCD}(13,23)=1$, le théorème de Gauss donne $23 \mid (x+7)$: il existe $k\in\mathbb{Z}$ tel que $x=23k-7$. En reportant, $13\times 23k=23(y+4)$, d'où $y=13k-4$.

$$\boxed{S=\{(23k-7\,;13k-4)\ ;\ k\in\mathbb{Z}\}}$$

Vérification : $13(23k-7)-23(13k-4)=299k-91-299k+92=1$.

EXERCICE 21 : POINTS ENTIERS D'UNE DROITE ⋆⋆

1. $7\times 1-4\times 1=3$: $\boxed{A\in\mathcal{D}}$
2. On cherche les couples d'entiers $(x\,;y)$ tels que $7x-4y=3$. En soustrayant $7\times 1-4\times 1=3$:

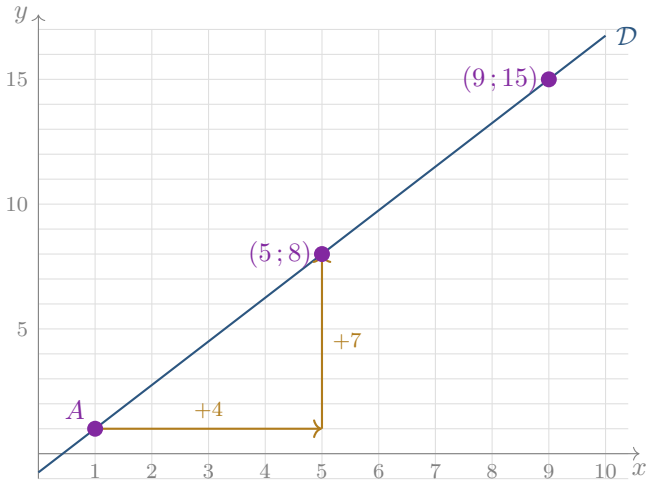
$$7(x-1)=4(y-1)$$

4 divise $7(x-1)$ et $\text{PGCD}(4,7)=1$, donc d'après le théorème de Gauss, $x-1=4k$ avec $k\in\mathbb{Z}$, puis $7\times 4k=4(y-1)$, d'où $y=1+7k$. La réciproque se vérifie : $7(1+4k)-4(1+7k)=7-4=3$.

$$\boxed{\text{Les points entiers de } \mathcal{D} \text{ sont les } M_k(1+4k\,;1+7k),\ k\in\mathbb{Z}}$$

3. $0\leqslant 1+4k\leqslant 20$ donne $-\frac{1}{4}\leqslant k\leqslant \frac{19}{4}$, soit $k\in\{0\,;1\,;2\,;3\,;4\}$, et alors $y=1+7k\geqslant 0$:

$$\boxed{(1\,;1),\ (5\,;8),\ (9\,;15),\ (13\,;22),\ (17\,;29)}$$



La droite bleu ardoise traverse le quadrillage, mais ne passe exactement par un nœud, c'est-à-dire par un point à coordonnées entières, qu'aux points violets. On passe de l'un au suivant en avançant de 4 et en montant de 7, comme le montrent les flèches ocre.

4. Deux points entiers consécutifs M_k et M_{k+1} sont séparés par le vecteur $\overrightarrow{M_kM_{k+1}}\begin{pmatrix}4\\7\end{pmatrix}$, qui ne dépend pas de k : ces points sont **régulièrement espacés**, à la distance $\sqrt{16+49}=\sqrt{65}$ les uns des autres. Le vecteur $\begin{pmatrix}4\\7\end{pmatrix}$ est un vecteur directeur de $\mathcal{D}$, à coordonnées entières et premières entre elles : il est le plus petit possible.

EXERCICE 22 ⋆⋆

1. C'est la question c) de l'exercice 10, valable ici pour tout entier relatif n :

$$5 \times (14n+3) - 14 \times (5n+1) = 70n + 15 - 70n - 14 = 1$$

D'après le théorème de Bézout : $\boxed{\forall n \in \mathbb{Z},\ \text{PGCD}(14n+3\,,\,5n+1) = 1}$

2. (a) Il suffit de choisir n tel que $14n+3 = 87$, c'est-à-dire $14n = 84$ et $n = 6$. On vérifie alors que $5 \times 6 + 1 = 31$.

$$\boxed{\text{87 et 31 sont premiers entre eux, d'après la question 1 avec } n = 6}$$

(b) La relation de la question 1, écrite pour $n = 6$, fournit directement le couple de Bézout :

$$5 \times 87 - 14 \times 31 = 435 - 434 = 1 \qquad \text{d'où} \qquad \boxed{(u\,;v) = (5\,;-14)}$$

On retrouve le couple déjà obtenu par la remontée de l'algorithme d'Euclide, à l'exercice 12 : la question 1 fournit ici le résultat sans aucun calcul.

En multipliant cette égalité par 2 :

$$87 \times 10 + 31 \times (-28) = 2 \qquad \text{d'où} \qquad \boxed{(x_0\,;y_0) = (10\,;-28)}$$

(c) Soit $(x\,;y)$ une solution de (E). En soustrayant terme à terme :

$$87(x-10) + 31(y+28) = 0 \qquad \text{soit} \qquad 87(x-10) = -31(y+28)$$

Comme 31 divise $87(x-10)$ et que $\text{PGCD}(87, 31) = 1$, le théorème de Gauss donne $31 \mid (x-10)$: il existe $k \in \mathbb{Z}$ tel que $x = 31k + 10$. En reportant, $87 \times 31k = -31(y+28)$, d'où $y = -87k - 28$.

$$\boxed{S = \{(31k+10\,;-87k-28)\ ;\ k \in \mathbb{Z}\}}$$

Vérification : $87(31k+10) + 31(-87k-28) = 2697k + 870 - 2697k - 868 = 2$.

3. L'équation de la droite s'écrit $87x - 31y = 2$. Attention : le signe a changé, il ne s'agit plus de (E). On repart du couple de Bézout $87 \times 5 - 31 \times 14 = 1$, que l'on multiplie par 2 :

$$87 \times 10 - 31 \times 28 = 2 \qquad \text{d'où la solution particulière } (10\,;28)$$

Soit $(x\,;y)$ une solution. En soustrayant terme à terme :

$$87(x-10) = 31(y-28)$$

Le théorème de Gauss donne $31 \mid (x-10)$, donc $x = 31k + 10$ et $y = 87k + 28$.

On cherche maintenant les points à coordonnées entières *naturelles* avec $0 \leqslant x \leqslant 10$. Comme $x = 31k + 10$:

$$0 \leqslant 31k + 10 \leqslant 10 \iff -10 \leqslant 31k \leqslant 0 \iff k = 0$$

et alors $y = 28 \geqslant 0$.

$$\boxed{\text{Le seul point convenable est } (10\,;28)}$$

Vérification : $87 \times 10 - 31 \times 28 - 2 = 870 - 868 - 2 = 0$.

EXERCICE 23 ⋆⋆

1. (a) PGCD$(8,5) = 1$ divise 1 : l'équation admet des solutions. On en cherche une évidente :

$$8 \times 2 + 5 \times (-3) = 16 - 15 = 1 \qquad \text{d'où} \qquad \boxed{(x_0\,;y_0) = (2\,;-3)}$$

   (b) Soit $(x\,;y)$ une solution. En soustrayant terme à terme :

$$8(x-2) + 5(y+3) = 0 \qquad \text{soit} \qquad 8(x-2) = -5(y+3)$$

Comme 5 divise $8(x-2)$ et que PGCD$(5,8) = 1$, le théorème de Gauss donne $5 \mid (x-2)$: il existe $k \in \mathbb{Z}$ tel que $x = 5k+2$. En reportant, $8 \times 5k = -5(y+3)$, d'où $y = -8k-3$.

$$\boxed{S = \{(5k+2\,;-8k-3)\ ;\ k \in \mathbb{Z}\}}$$

Vérification : $8(5k+2) + 5(-8k-3) = 40k + 16 - 40k - 15 = 1$.

2. (a) Les deux écritures de n donnent $8a + 1 = 5b + 2$, c'est-à-dire :

$$8a - 5b = 1 \qquad \text{soit} \qquad 8a + 5 \times (-b) = 1$$

$$\boxed{\text{Le couple } (a\,;-b) \text{ est bien solution de } (E)}$$

   (b) D'après la question 1b, il existe $k \in \mathbb{Z}$ tel que :

$$a = 5k + 2 \qquad \text{et} \qquad -b = -8k - 3, \text{ soit } b = 8k + 3$$

On en déduit :

$$n = 8a + 1 = 8(5k+2) + 1 = 40k + 17$$

Comme $0 \leqslant 17 < 40$:

$$\boxed{\text{Le reste de la division euclidienne de } n \text{ par } 40 \text{ est } 17}$$

Vérification avec $k = 0$: $n = 17$, et l'on a bien $17 = 8 \times 2 + 1 = 5 \times 3 + 2$.

3. (a) PGCD$(8,5) = 1$ divise 100 : l'équation admet des solutions. Une solution évidente saute aux yeux :

$$8 \times 0 + 5 \times 20 = 100 \qquad \text{d'où} \qquad (x_0\,;y_0) = (0\,;20)$$

Soit $(x\,;y)$ une solution. En soustrayant terme à terme :

$$8x + 5(y-20) = 0 \qquad \text{soit} \qquad 8x = 5(20-y)$$

Comme 5 divise $8x$ et que PGCD$(5,8) = 1$, le théorème de Gauss donne $5 \mid x$: il existe $k \in \mathbb{Z}$ tel que $x = 5k$. En reportant, $8 \times 5k = 5(20-y)$, d'où $y = 20 - 8k$.

$$\boxed{S = \{(5k\,;20-8k)\ ;\ k \in \mathbb{Z}\}}$$

Vérification : $8 \times 5k + 5(20-8k) = 40k + 100 - 40k = 100$.

(b) Notons x le nombre d'hommes et y celui de femmes. La dépense totale s'écrit $8x+5y=100$, et ces deux nombres doivent être des entiers **naturels**. On impose donc :

$$\begin{cases} 5k \geqslant 0 \\ 20-8k \geqslant 0 \end{cases} \qquad \text{soit} \qquad 0 \leqslant k \leqslant \frac{20}{8} = 2{,}5$$

Les valeurs possibles sont $k \in \{0\,;1\,;2\}$:

k	0	1	2
Nombre d'hommes	0	5	10
Nombre de femmes	20	12	4

L'énoncé parle d'un groupe *d'hommes et de femmes* : les deux nombres doivent être non nuls, ce qui écarte $k=0$.

Soit 5 hommes et 12 femmes, soit 10 hommes et 4 femmes

Vérification : $5\times 8+12\times 5=40+60=100$ et $10\times 8+4\times 5=80+20=100$.

EXERCICE 24 : À LA FERME ⋆⋆

1. La dépense s'écrit $7x+11y=200$, avec x et y entiers naturels non nuls.
2. Algorithme d'Euclide : $11=7\times 1+4$, $7=4\times 1+3$, $4=3\times 1+1$. Remontée :

$$1=4-3=4-(7-4)=2\times 4-7=2\times(11-7)-7=2\times 11-3\times 7$$

Ainsi $7\times(-3)+11\times 2=1$, et en multipliant par 200 :

$$7\times(-600)+11\times 400=200 \qquad \text{d'où la solution particulière} \qquad (-600\,;400)$$

3. Si $(x\,;y)$ est solution, en soustrayant : $7(x+600)=11(400-y)$. Comme 11 divise $7(x+600)$ et que $\text{PGCD}(7,11)=1$, le théorème de Gauss donne $x+600=11k$, puis $y=400-7k$, avec $k\in\mathbb{Z}$. La réciproque se vérifie : $7(11k-600)+11(400-7k)=-4200+4400=200$.

$$S=\{(11k-600\,;400-7k)\ ;\ k\in\mathbb{Z}\}$$

On impose $x\geqslant 1$ et $y\geqslant 1$:

$$11k\geqslant 601 \iff k\geqslant 54{,}6\ldots \qquad ; \qquad 7k\leqslant 399 \iff k\leqslant 57$$

donc $k\in\{55\,;56\,;57\}$:

k	55	56	57
Poules	5	16	27
Lapins	15	8	1

3 achats possibles : 5 poules et 15 lapins, 16 et 8, ou 27 et 1

Vérification : $35+165=112+88=189+11=200$. La solution particulière obtenue par la remontée est très éloignée des solutions utiles : il ne faut pas s'en inquiéter, la solution générale permet de revenir dans le bon domaine.

EXERCICE 25 ⋆⋆⋆

Notons a le nombre d'adultes payant plein tarif, e celui des étudiants et f celui des enfants. L'énoncé se traduit par le système :

$$\begin{cases} a+e+f=28 \\ 26a+17e+13f=613 \end{cases}$$

On élimine a en remplaçant $a=28-e-f$ dans la seconde équation :

$$\begin{aligned} 26(28-e-f)+17e+13f &= 613 \\ 728-26e-26f+17e+13f &= 613 \\ -9e-13f &= -115 \end{aligned}$$

$$\boxed{9e+13f=115}$$

Il reste à résoudre cette équation diophantienne. Comme $\text{PGCD}(9,13)=1$ divise 115, elle admet des solutions.

Solution particulière. On cherche d'abord un couple de Bézout pour 9 et 13 :

$$9\times 3-13\times 2=27-26=1$$

En multipliant par 115 :

$$9\times 345+13\times(-230)=115 \qquad \text{d'où} \qquad (e_0\,;f_0)=(345\,;-230)$$

Solutions générales. Soit $(e\,;f)$ une solution. En soustrayant terme à terme :

$$9(e-345)+13(f+230)=0 \qquad \text{soit} \qquad 9(e-345)=-13(f+230)$$

Comme 13 divise $9(e-345)$ et que $\text{PGCD}(9,13)=1$, le théorème de Gauss donne $13\mid(e-345)$: il existe $k\in\mathbb{Z}$ tel que $e=13k+345$. En reportant, $9\times 13k=-13(f+230)$, d'où $f=-9k-230$.

Contraintes du problème. Les trois effectifs sont des entiers naturels :

$$\begin{cases} e=13k+345\geqslant 0 \\ f=-9k-230\geqslant 0 \\ a=28-e-f\geqslant 0 \end{cases} \qquad \text{soit} \qquad \begin{cases} k\geqslant -\frac{345}{13}\approx -26{,}5 \\ k\leqslant -\frac{230}{9}\approx -25{,}6 \\ 28-(13k+345)-(-9k-230)\geqslant 0 \end{cases}$$

Les deux premières conditions imposent $-26{,}5\leqslant k\leqslant -25{,}6$, donc $k=-26$. On obtient alors :

$$e=13\times(-26)+345=-338+345=7 \qquad ; \qquad f=-9\times(-26)-230=234-230=4$$

puis $a=28-7-4=17$. La troisième condition est bien vérifiée.

$$\boxed{\text{17 adultes, 7 étudiants et 4 enfants}}$$

Vérification : $17+7+4=28$ et $26\times 17+17\times 7+13\times 4=442+119+52=613$.

EXERCICE 26 : THÉORÈME DES RESTES CHINOIS ⋆⋆

1. (a) Les nombres 17 et 5 sont deux nombres premiers distincts, donc $\text{PGCD}(17, 5) = 1$. D'après le théorème de Bézout :

$$\boxed{\text{Il existe un couple } (u\,;v) \text{ d'entiers relatifs tel que } 17u + 5v = 1}$$

(b) Montrons que $n_0 = 3 \times 17u + 9 \times 5v$ vérifie les deux congruences.

Modulo 17 : le terme $3 \times 17u$ est un multiple de 17, donc $n_0 \equiv 9 \times 5v$ [17]. Or l'égalité $17u + 5v = 1$ donne $5v \equiv 1$ [17], d'où :

$$n_0 \equiv 9 \times 1 \equiv 9 \text{ [17]}$$

Modulo 5 : le terme $9 \times 5v$ est un multiple de 5, donc $n_0 \equiv 3 \times 17u$ [5]. Or $17u \equiv 1$ [5], d'où :

$$n_0 \equiv 3 \times 1 \equiv 3 \text{ [5]}$$

$$\boxed{n_0 \text{ appartient à } S}$$

(c) Cherchons un couple de Bézout. Comme $17 = 5 \times 3 + 2$ et $5 = 2 \times 2 + 1$, la remontée donne :

$$\begin{aligned} 1 &= 5 - 2 \times 2 \qquad\qquad \text{or } 2 = 17 - 5 \times 3 \\ &= 5 - (17 - 5 \times 3) \times 2 \\ &= 5 - 17 \times 2 + 5 \times 6 \\ &= 17 \times (-2) + 5 \times 7 \end{aligned}$$

On peut donc prendre $(u\,;v) = (-2\,;7)$. Alors :

$$n_0 = 3 \times 17 \times (-2) + 9 \times 5 \times 7 = -102 + 315 = 213$$

On vérifie : $213 = 17 \times 12 + 9$ et $213 = 5 \times 42 + 3$.

$$\boxed{n_0 = 213 \text{ convient}}$$

2. (a) Soit $n \in S$. Alors $n \equiv 9$ [17] et $n_0 \equiv 9$ [17], donc par différence $n - n_0 \equiv 0$ [17] : le nombre 17 divise $n - n_0$. De même, $n \equiv 3$ [5] et $n_0 \equiv 3$ [5] donnent que 5 divise $n - n_0$.

Ainsi 17 et 5 divisent tous deux $n - n_0$, et ils sont premiers entre eux. D'après le **corollaire du théorème de Gauss**, leur produit divise également $n - n_0$:

$$\boxed{n - n_0 \equiv 0 \text{ [85]}}$$

(b) D'après ce qui précède, il existe $k \in \mathbb{Z}$ tel que $n = n_0 + 85k = 213 + 85k$. Or $213 = 85 \times 2 + 43$, donc en posant $k' = k + 2$:

$$n = 43 + 85k'$$

Réciproquement, tout entier de cette forme vérifie $n \equiv 43 \equiv 9$ [17] (car $43 = 17 \times 2 + 9$) et $n \equiv 43 \equiv 3$ [5] (car $43 = 5 \times 8 + 3$), donc appartient bien à S.

$$\boxed{S = \{43 + 85k\ ;\ k \in \mathbb{Z}\}}$$

3. Le nombre N de jetons vérifie $N \equiv 9\ [17]$ et $N \equiv 3\ [5]$: il appartient donc à S, et s'écrit $N = 43 + 85k$. La condition $300 \leqslant N \leqslant 400$ donne :

$$300 \leqslant 43 + 85k \leqslant 400 \iff 257 \leqslant 85k \leqslant 357 \iff 3{,}02 \leqslant k \leqslant 4{,}2$$

Le seul entier convenable est $k = 4$:

$$N = 43 + 85 \times 4 = 43 + 340 = \boxed{383 \text{ jetons}}$$

Vérification : $383 = 17 \times 22 + 9$ et $383 = 5 \times 76 + 3$.

EXERCICE 27 : RESTES CHINOIS AVEC DES MODULES NON PREMIERS ENTRE EUX ⋆⋆⋆

1. Si $n \equiv 1\ [6]$, alors $n = 6q + 1$ est impair. Si $n \equiv 4\ [8]$, alors $n = 8q' + 4$ est pair. Un entier ne peut pas être à la fois pair et impair :

$$\boxed{\text{le système } n \equiv 1\ [6],\ n \equiv 4\ [8] \text{ n'a aucune solution}}$$

2. (a) $n \equiv 3\ [6]$ signifie qu'il existe $a \in \mathbb{Z}$ tel que $n = 6a + 3$, et $n \equiv 5\ [8]$ qu'il existe $b \in \mathbb{Z}$ tel que $n = 8b + 5$. Alors $6a + 3 = 8b + 5$, soit $6a - 8b = 2$, et en divisant par 2 : $\boxed{3a - 4b = 1}$.

   (b) Le couple $(3\,;2)$ est solution, car $9 - 8 = 1$. En soustrayant : $3(a - 3) = 4(b - 2)$. Par le théorème de Gauss, $a - 3 = 4k$ avec $k \in \mathbb{Z}$, puis $b = 2 + 3k$. Alors :

$$n = 6(3 + 4k) + 3 = 21 + 24k$$

   Réciproquement, si $n = 21 + 24k$, alors $n = 6(3+4k)+3 \equiv 3\ [6]$ et $n = 8(2+3k)+5 \equiv 5\ [8]$.

$$\boxed{n \equiv 3\ [6] \text{ et } n \equiv 5\ [8] \iff n \equiv 21\ [24]}$$

3. Dans l'exercice 26, les modules 17 et 5 sont premiers entre eux. Le corollaire de Gauss (Proposition 6) permettait alors de passer de « 17 et 5 divisent $n - n_0$ » à « 85 divise $n - n_0$ ». Ici, 6 et 8 ne sont pas premiers entre eux, et la Proposition 6 ne s'applique pas : 6 et 8 divisent $45 - 21 = 24$, mais 48 ne divise pas 24. Le bon module est 24, le plus petit multiple commun de 6 et 8 (voir l'exercice 29). Selon les restes imposés, le système peut alors n'avoir aucune solution (question 1), ou des solutions qui se répètent modulo 24 (question 2).

EXERCICE 28 ⋆⋆

1. (a)

$$u_1 = 4 \times 0 + 1 = \boxed{1} \quad ; \quad u_2 = 4 \times 1 + 1 = \boxed{5} \quad ; \quad u_3 = 4 \times 5 + 1 = \boxed{21}$$

   (b) Soit $n \in \mathbb{N}$. La relation de récurrence s'écrit :

$$u_{n+1} - 4u_n = 1 \qquad \text{c'est-à-dire} \qquad 1 \times u_{n+1} + (-4) \times u_n = 1$$

   C'est une combinaison linéaire de u_{n+1} et u_n à coefficients entiers, égale à 1. D'après le théorème de Bézout :

$$\boxed{u_{n+1} \text{ et } u_n \text{ sont premiers entre eux}}$$

2. (a) Pour tout $n \in \mathbb{N}$:

$$\begin{aligned} v_{n+1} &= u_{n+1} + \frac{1}{3} = 4u_n + 1 + \frac{1}{3} = 4u_n + \frac{4}{3} \\ &= 4\left(u_n + \frac{1}{3}\right) = 4v_n \end{aligned}$$

$$\boxed{(v_n) \text{ est géométrique de raison 4 et de premier terme } v_0 = \frac{1}{3}}$$

(b) On en déduit $v_n = \dfrac{1}{3} \times 4^n$, puis :

$$u_n = v_n - \frac{1}{3} = \frac{4^n}{3} - \frac{1}{3}$$

$$\boxed{u_n = \frac{4^n - 1}{3}}$$

Vérification : $u_3 = \dfrac{64-1}{3} = 21$.

3. L'expression précédente donne $4^n - 1 = 3u_n$ et $4^{n+1} - 1 = 3u_{n+1}$. Or le PGCD est compatible avec la multiplication par un entier positif :

$$\text{PGCD}\left(4^{n+1} - 1\,,\, 4^n - 1\right) = \text{PGCD}\left(3u_{n+1}\,,\, 3u_n\right) = 3 \times \text{PGCD}(u_{n+1}, u_n)$$

Or la question 1b a établi que $\text{PGCD}(u_{n+1}, u_n) = 1$:

$$\boxed{\text{PGCD}\left(4^{n+1} - 1\,,\, 4^n - 1\right) = 3}$$

Vérification pour $n = 2$: $\text{PGCD}(63, 15) = 3$.

EXERCICE 29 : PGCD ET PPCM ⋆⋆⋆

1. Soit δ un diviseur commun positif de a' et b'. Alors $d\delta$ divise $da' = a$ et $db' = b$: c'est un diviseur commun de a et b, donc $d\delta \leqslant d$, d'où $\delta \leqslant 1$. Ainsi $\boxed{\text{PGCD}(a', b') = 1}$. C'est aussi une conséquence de la Proposition 3 : $d = \text{PGCD}(da', db') = d \times \text{PGCD}(a', b')$.
2. $m = da'b' = a \times b' = b \times a'$: m est bien un multiple de a et de b.
3. $M = ak = da'k$ est un multiple de $b = db'$: il existe j tel que $da'k = db'j$, soit $a'k = b'j$. Ainsi b' divise $a'k$; comme $\text{PGCD}(a', b') = 1$, le théorème de Gauss donne $b' \mid k$. En écrivant $k = b'k'$:

$$M = ab'k' = m\,k' \qquad \text{donc} \qquad m \mid M$$

4. m est un multiple commun non nul de a et b. Si M est un autre multiple commun positif, m divise M d'après la question 3, donc $m \leqslant M$. Ainsi m est le plus petit :

$$\boxed{\text{PPCM}(a, b) = da'b'}$$

puis $d \times da'b' = (da')(db') = ab$, soit :

$$\boxed{\text{PGCD}(a, b) \times \text{PPCM}(a, b) = ab}$$

5. À chaque dent qui passe, chaque roue avance d'une dent. Les deux points rouges se retrouvent face à face lorsque le nombre N de dents passées est à la fois un multiple de 36, pour que la première roue ait fait un nombre entier de tours, et de 60, pour la seconde. Le premier tel N est :

$$N = \text{PPCM}(36, 60) = \frac{36 \times 60}{\text{PGCD}(36, 60)} = \frac{2160}{12} = 180$$

$$\boxed{\text{la première roue fait } \tfrac{180}{36} = 5 \text{ tours, la seconde } \tfrac{180}{60} = 3 \text{ tours}}$$

EXERCICE 30 : NOMBRES DE FERMAT ⋆⋆

1. (a) On développe le produit du membre de droite. En notant $S = x^{2k} - x^{2k-1} + \cdots + x^2 - x + 1$, la somme alternée des puissances de x de 0 à $2k$:

$$(x+1)S = \underbrace{\left(x^{2k+1} - x^{2k} + \cdots + x^3 - x^2 + x\right)}_{x \times S} + \underbrace{\left(x^{2k} - x^{2k-1} + \cdots + x^2 - x + 1\right)}_{S}$$

Tous les termes intermédiaires s'éliminent deux à deux, car ils apparaissent une fois avec chaque signe. Il ne reste que le premier terme de la première somme et le dernier de la seconde :

$$\boxed{x^{2k+1} + 1 = (x+1)\left(x^{2k} - x^{2k-1} + \cdots + x^2 - x + 1\right)}$$

C'est le télescopage classique de la somme géométrique de raison $-x$.

(b) Soit m un entier impair, $m \geqslant 3$. On écrit $m = 2k+1$ avec $k \geqslant 1$, et l'on applique l'égalité précédente à $x = 2$:

$$2^m + 1 = (2+1) \times S = 3S$$

Le nombre $2^m + 1$ est donc divisible par 3. Comme $m \geqslant 3$, on a $2^m + 1 \geqslant 9 > 3$:

$$\boxed{2^m + 1 \text{ n'est pas premier}}$$

Le cas $m = 1$ est à écarter : $2^1 + 1 = 3$ est bien premier.

(c) Supposons que m possède un diviseur strict impair $d > 1$, et écrivons $m = dq$ avec $q \geqslant 1$. En posant $x = 2^q$ et $d = 2k+1$, l'égalité de la question a) donne :

$$2^m + 1 = (2^q)^d + 1 = x^d + 1 = (x+1) \times S = (2^q + 1) \times S$$

Le nombre $2^q + 1$ est donc un diviseur de $2^m + 1$. Il est strictement supérieur à 1 puisque $q \geqslant 1$, et strictement inférieur à $2^m + 1$ puisque $q < m$ (car $d > 1$).

$$\boxed{2^m + 1 \text{ n'est pas premier}}$$

(d) Soit $m \geqslant 1$ tel que $2^m + 1$ soit premier. D'après la question c), m ne possède aucun diviseur impair strictement supérieur à 1. Or tout entier s'écrit comme un produit de nombres premiers : si l'un d'eux était impair, il fournirait un tel diviseur. Tous les facteurs premiers de m valent donc 2 :

$$\boxed{m \text{ est une puissance de 2, donc } 2^m + 1 = 2^{2^n} + 1}$$

2. (a)

$$F_0 = 2^1 + 1 = \boxed{3} \quad ; \quad F_1 = 2^2 + 1 = \boxed{5} \quad ; \quad F_2 = 2^4 + 1 = \boxed{17}$$
$$F_3 = 2^8 + 1 = \boxed{257} \quad ; \quad F_4 = 2^{16} + 1 = \boxed{65\,537}$$

Les nombres 3, 5, 17 et 257 se testent rapidement. Pour 65 537, il suffit de tester les diviseurs premiers jusqu'à $\sqrt{65\,537} \approx 256$:

$$\boxed{F_0,\ F_1,\ F_2,\ F_3 \text{ et } F_4 \text{ sont tous premiers}}$$

(b)

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297$$

Un test de primalité montre que ce nombre **n'est pas premier** :

$$\boxed{F_5 = 641 \times 6\,700\,417}$$

La conjecture de Fermat est donc fausse. C'est Euler qui trouva cette factorisation en 1732, près d'un siècle après Fermat. On ne connaît d'ailleurs aujourd'hui aucun nombre de Fermat premier au-delà de F_4.

(c) Par définition, $F_n - 1 = 2^{2^n}$, donc :

$$(F_n - 1)^2 + 1 = \left(2^{2^n}\right)^2 + 1 = 2^{2\times 2^n} + 1 = 2^{2^{n+1}} + 1 = F_{n+1}$$

$$\boxed{F_{n+1} = (F_n - 1)^2 + 1}$$

En développant, $F_{n+1} = F_n^2 - 2F_n + 2$, donc :

$$F_{n+1} \equiv 2\ [F_n]$$

Ainsi $\text{PGCD}(F_n, F_{n+1}) = \text{PGCD}(F_n, 2)$. Or $F_n = 2^{2^n} + 1$ est impair :

$$\boxed{\text{PGCD}(F_n, F_{n+1}) = 1}$$

Deux nombres de Fermat consécutifs sont donc toujours premiers entre eux.

3. Démontrons par récurrence la propriété $\mathcal{P}(n)$: « F_n se termine par le chiffre 7 », pour $n \geqslant 2$.

Initialisation : $F_2 = 17$ se termine bien par 7, donc $\mathcal{P}(2)$ est vraie.

Hérédité : Supposons $\mathcal{P}(n)$ vraie pour un entier $n \geqslant 2$, c'est-à-dire $F_n \equiv 7\ [10]$. Alors $F_n - 1 \equiv 6\ [10]$, et d'après la question 2c :

$$F_{n+1} = (F_n - 1)^2 + 1 \equiv 6^2 + 1 = 37 \equiv 7\ [10]$$

Donc $\mathcal{P}(n+1)$ est vraie.

Conclusion : La propriété est vraie au rang 2 et héréditaire :

$$\boxed{\text{Pour tout } n \geqslant 2,\ F_n \text{ se termine par le chiffre 7}}$$

On le vérifie : $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$, $F_5 = 4\,294\,967\,297$.

EXERCICE 31 : CRYPTAGE RSA ⋆⋆

1. (a) On calcule les puissances de 8 modulo 55 de proche en proche :

$$8^2 = 64 \equiv 9\ [55] \quad ; \quad 8^4 \equiv 9^2 = 81 \equiv 26\ [55]$$

$$8^6 \equiv 26 \times 9 = 234 = 4 \times 55 + 14 \equiv 14\ [55]$$

$$8^7 \equiv 14 \times 8 = 112 = 2 \times 55 + 2 \equiv 2\ [55]$$

$$\boxed{8^7 \equiv 2\ [55]}$$

On en déduit, en élevant au cube :

$$8^{21} = \left(8^7\right)^3 \equiv 2^3 = 8\ [55]$$

$$\boxed{\text{Le reste de la division euclidienne de } 8^{21} \text{ par 55 est 8}}$$

(b) Le premier calcul ci-dessus donne $\boxed{8^2 \equiv 9\ [55]}$. On décompose alors :

$$8^{23} = 8^{21} \times 8^2 \equiv 8 \times 9 = 72 = 55 + 17 \equiv 17\ [55]$$

$$\boxed{\text{Le reste de la division euclidienne de } 8^{23} \text{ par 55 est 17}}$$

2. (a) PGCD$(23, 40) = 1$ car 23 est premier et ne divise pas 40. Comme 1 divise 1, le corollaire de Bézout garantit :

$$\boxed{\text{L'équation } (E) \text{ admet au moins un couple solution}}$$

(b) On cherche un couple par l'algorithme d'Euclide :

$$\begin{aligned} 40 &= 23 \times 1 + 17 \qquad (L_1) \\ 23 &= 17 \times 1 + 6 \qquad (L_2) \\ 17 &= 6 \times 2 + 5 \qquad (L_3) \\ 6 &= 5 \times 1 + 1 \qquad (L_4) \end{aligned}$$

Remontée :

$$\begin{aligned} 1 &= 6 - 5 \times 1 && \text{or } (L_3) : \ 5 = 17 - 6 \times 2 \\ &= 6 - (17 - 6 \times 2) = 3 \times 6 - 17 && \text{or } (L_2) : \ 6 = 23 - 17 \\ &= 3 \times (23 - 17) - 17 = 3 \times 23 - 4 \times 17 && \text{or } (L_1) : \ 17 = 40 - 23 \\ &= 3 \times 23 - 4 \times (40 - 23) = 7 \times 23 - 4 \times 40 \end{aligned}$$

$$\boxed{(x_0\,;y_0) = (7\,;4) \quad \text{car} \quad 23 \times 7 - 40 \times 4 = 161 - 160 = 1}$$

(c) Soit $(x\,;y)$ une solution. En soustrayant terme à terme :

$$23(x-7) - 40(y-4) = 0 \qquad \text{soit} \qquad 23(x-7) = 40(y-4)$$

Comme 40 divise $23(x-7)$ et que PGCD$(23, 40) = 1$, le théorème de Gauss donne $40 \mid (x-7)$: il existe $k \in \mathbb{Z}$ tel que $x = 40k + 7$. En reportant, $23 \times 40k = 40(y-4)$, d'où $y = 23k + 4$.

$$\boxed{S = \{(40k+7\,;23k+4)\ ;\ k \in \mathbb{Z}\}}$$

Vérification : $23(40k+7) - 40(23k+4) = 920k + 161 - 920k - 160 = 1$.

(d) Dire que $23d \equiv 1\ [40]$ signifie que 40 divise $23d - 1$, c'est-à-dire qu'il existe un entier y tel que $23d - 40y = 1$: le couple $(d\,;y)$ est solution de (E). D'après la question c), d s'écrit $d = 40k + 7$. La condition $0 \leqslant d < 40$ impose alors $k = 0$.

$$\boxed{d = 7 \text{ est l'unique entier vérifiant les deux conditions}}$$

3. (a)

$$N = p \times q = 5 \times 11 = \boxed{55} \qquad ; \qquad n = (p-1)(q-1) = 4 \times 10 = \boxed{40}$$

Il reste à vérifier que $c = 23$ est premier avec $n = 40$, ce qui a été établi à la question 2a :

$$\boxed{\text{PGCD}(23, 40) = 1 : \text{la condition est bien remplie}}$$

(b) Le nombre crypté b est le reste de la division euclidienne de $a^c = 8^{23}$ par $N = 55$. C'est exactement le calcul de la question 1b :

$$\boxed{b = 17}$$

4. (a) L'entier d doit vérifier $0 \leqslant d < n = 40$ et $cd = 23d \equiv 1\ [40]$: c'est précisément la caractérisation de la question 2d.

$$\boxed{d = 7}$$

(b) On calcule le reste de $b^d = 17^7$ modulo 55, de proche en proche :

$$17^2 = 289 = 5 \times 55 + 14 \equiv 14\ [55]$$

$$17^4 \equiv 14^2 = 196 = 3 \times 55 + 31 \equiv 31\ [55]$$

$$17^6 \equiv 31 \times 14 = 434 = 7 \times 55 + 49 \equiv 49\ [55]$$

$$17^7 \equiv 49 \times 17 = 833 = 15 \times 55 + 8 \equiv 8\ [55]$$

$$\boxed{a = 8}$$

On retrouve bien le nombre initial de la question 3b : le décryptage fonctionne.

Toute la sécurité du procédé repose sur le fait que d se calcule à partir de $n = (p-1)(q-1)$, donc de la factorisation $N = p \times q$. Avec $N = 55$, cette factorisation est immédiate ; avec un N de plusieurs centaines de chiffres, elle est hors de portée des ordinateurs actuels.

Pour aller plus loin

EXERCICE 32 ⋆⋆

On élimine n en combinant les deux nombres avec les coefficients 3 et -2, car $3 \times 14 = 2 \times 21 = 42$:

$$3(14n + 3) - 2(21n + 4) = 42n + 9 - 42n - 8 = 1$$

$$\boxed{3 \times (14n + 3) + (-2) \times (21n + 4) = 1}$$

C'est une relation de Bézout. D'après le théorème de Bézout, $14n + 3$ et $21n + 4$ sont premiers entre eux pour tout $n \in \mathbb{N}$.

EXERCICE 33 ⋆⋆

Pour $n \in \mathbb{N}$, notons $\mathcal{P}_n$: « $\text{PGCD}(F_n, F_{n+1}) = 1$ ».

Initialisation : $\text{PGCD}(F_0, F_1) = \text{PGCD}(0, 1) = 1$, d'après la Proposition 1.

Hérédité : Supposons $\mathcal{P}_n$ vraie. Un diviseur commun de F_{n+1} et F_{n+2} divise $F_{n+2} - F_{n+1} = F_n$; réciproquement, un diviseur commun de F_n et F_{n+1} divise $F_n + F_{n+1} = F_{n+2}$. Les deux couples ont donc les mêmes diviseurs communs, d'où :

$$\text{PGCD}(F_{n+1}, F_{n+2}) = \text{PGCD}(F_n, F_{n+1}) = 1$$

Conclusion : Pour tout $n \in \mathbb{N}$: $\boxed{\text{PGCD}(F_n, F_{n+1}) = 1}$

Deux termes consécutifs de la suite de Fibonacci sont toujours premiers entre eux. L'algorithme d'Euclide appliqué à F_{n+1} et F_n ne fait que redescendre la suite, avec des quotients tous égaux à 1 : c'est le cas où il est le plus lent.

EXERCICE 34 ⋆⋆

- Si n est premier. Soit $a \in \{1, \dots, n-1\}$. Les seuls diviseurs positifs de n sont 1 et n, et n ne divise pas a puisque $0 < a < n$. Donc $\text{PGCD}(a, n) = 1$, et le théorème de Bézout fournit u, v entiers tels que $au + nv = 1$. Ainsi $au \equiv 1\ [n]$: u est un inverse de a modulo n.
- Si n n'est pas premier. On écrit $n = rs$ avec $1 < r < n$, de sorte que $r \in \{1, \dots, n-1\}$. Supposons que $rx \equiv 1\ [n]$ pour un entier x. Alors n divise $rx - 1$, donc r aussi ; comme r divise rx, il divise $rx - (rx - 1) = 1$, ce qui contredit $r > 1$. L'entier r n'a donc pas d'inverse modulo n.

$$\boxed{n \text{ est premier } \iff \text{ tout élément de } \{1, \dots, n-1\} \text{ admet un inverse modulo } n}$$

Par exemple, modulo 26, l'entier 13 n'a pas d'inverse : c'est la question 3c de l'exercice 13.

EXERCICE 35 ⋆⋆⋆

- Sens direct. Supposons $\text{PGCD}(a,b)=1$, et supposons par l'absurde que $\text{PGCD}(a+b,ab)>1$. Ce PGCD admet alors un diviseur premier p, qui divise ab et $a+b$. D'après le lemme d'Euclide (chapitre 1), p divise a ou b. Si $p \mid a$, alors $p \mid (a+b)-a=b$; si $p \mid b$, alors $p \mid a$ de même. Dans les deux cas, p est un diviseur commun de a et b supérieur à 1 : c'est absurde.
- Réciproque. Soit $d=\text{PGCD}(a,b)$. Il divise $a+b$ et ab, donc il divise $\text{PGCD}(a+b,ab)=1$ d'après la Proposition 4. D'où $d=1$.

$$\boxed{\text{PGCD}(a,b)=1 \iff \text{PGCD}(a+b,ab)=1}$$

Le passage par un diviseur premier est commode : être premiers entre eux, c'est n'avoir aucun facteur premier en commun.

EXERCICE 36 ⋆⋆⋆

a) Soit $(u\,;v)$ un couple de Bézout : $au+bv=1$. Montrons par récurrence sur $k \geqslant 1$ qu'il existe des entiers u_k et v_k tels que $a^k u_k + bv_k = 1$.
Initialisation : Pour $k=1$, on prend $u_1=u$ et $v_1=v$.
Hérédité : Si $a^k u_k + bv_k = 1$, on multiplie membre à membre par $au+bv=1$:

$$1=(a^k u_k+bv_k)(au+bv)=a^{k+1}(u_k u)+b\left(a^k u_k v+auv_k+bv_k v\right)$$

ce qui fournit $u_{k+1}=u_k u$ et $v_{k+1}=a^k u_k v+auv_k+bv_k v$, entiers.
Conclusion : D'après le théorème de Bézout, a^k et b sont premiers entre eux pour tout $k \in \mathbb{N}^*$.

b) D'après a), a^k et b sont premiers entre eux. On applique à nouveau a) au couple $(b\,;a^k)$ et à l'exposant ℓ : b^ℓ et a^k sont premiers entre eux.

$$\boxed{\text{PGCD}\left(a^k,b^\ell\right)=1}$$

EXERCICE 37 ⋆⋆⋆

Comme $u \geqslant 2$ et $v \geqslant 2$, on a $\ln(u)>0$ et $\ln(v)>0$: le quotient est bien défini et strictement positif. Supposons par l'absurde qu'il soit rationnel : $\dfrac{\ln(v)}{\ln(u)}=\dfrac{p}{q}$ avec p et q dans $\mathbb{N}^*$. Alors :

$$q\ln(v)=p\ln(u) \iff \ln\left(v^q\right)=\ln\left(u^p\right) \iff v^q=u^p$$

car la fonction ln est strictement croissante. Comme $u \geqslant 2$, u admet un diviseur premier r. Alors r divise $u^p=v^q$, donc, d'après le lemme d'Euclide (chapitre 1), r divise v. Ainsi r est un diviseur commun de u et v supérieur à 1, ce qui contredit $\text{PGCD}(u,v)=1$.

$$\boxed{\frac{\ln(v)}{\ln(u)} \text{ est irrationnel}}$$

Par exemple, $\dfrac{\ln(3)}{\ln(2)}$ est irrationnel. C'est pourquoi aucune puissance de 3 n'est une puissance de 2, ce qui revient à dire, en musique, qu'aucune succession de quintes justes ne retombe exactement sur une octave.

EXERCICE 38 : RACINES RATIONNELLES D'UN POLYNÔME ⋆⋆⋆

a) $P\left(\frac{p}{q}\right) = 0$ s'écrit, après multiplication par q^n :

$$\sum_{k=0}^{n} a_k p^k q^{n-k} = 0$$

On isole le terme $k = n$:

$$a_n p^n = -\sum_{k=0}^{n-1} a_k p^k q^{n-k} = -q \sum_{k=0}^{n-1} a_k p^k q^{n-k-1}$$

car $n - k \geqslant 1$ pour $k \leqslant n-1$. Donc q divise $a_n p^n$. Comme p et q sont premiers entre eux, q et p^n le sont aussi (exercice 36), et le théorème de Gauss donne $\boxed{q \mid a_n}$.

De même, en isolant le terme $k = 0$: $a_0 q^n = -p \sum_{k=1}^{n} a_k p^{k-1} q^{n-k}$, donc p divise $a_0 q^n$. Comme p et q^n sont premiers entre eux, $\boxed{p \mid a_0}$.

b) $\sqrt{2}$ est racine de $P(x) = x^2 - 2$, avec $a_2 = 1$ et $a_0 = -2$. Si P avait une racine rationnelle $\frac{p}{q}$ sous forme irréductible, on aurait $q \mid 1$, donc $q = 1$, et $p \mid 2$: la racine serait un entier parmi ± 1 et ± 2. Or leurs carrés valent 1 ou 4, et non 2. Ainsi P n'a pas de racine rationnelle, et $\boxed{\sqrt{2} \text{ est irrationnel}}$.

c) Soit $P(x) = x^5 - 5x + 7$. On a $P'(x) = 5x^4 - 5 = 5(x^2-1)(x^2+1)$, du signe de $x^2 - 1$.

x	$-\infty$		-1		1		$+\infty$
$P'(x)$		$+$	0	$-$	0	$+$	
P	$-\infty$	↗	11	↘	3	↗	$+\infty$

Sur $[-1\,;+\infty[$, le minimum de P est $P(1) = 3 > 0$: il n'y a pas de racine. Sur $]-\infty\,;-1]$, P est continue et strictement croissante, avec $\lim\limits_{x\to-\infty} P(x) = -\infty$ et $P(-1) = 11 > 0$. D'après le théorème des valeurs intermédiaires, appliqué à une fonction strictement monotone, l'équation $P(x) = 0$ y a une unique solution α, et $\alpha < -1$.
Si α était rationnel, d'après a), ce serait un entier $(q \mid 1)$ divisant 7, donc $\alpha \in \{-7\,;-1\,;1\,;7\}$. Or $P(-7) = -16\,765$, $P(-1) = 11$, $P(1) = 3$ et $P(7) = 16\,779$: aucun n'est nul.

$$\boxed{\text{l'unique solution réelle de } x^5 - 5x + 7 = 0 \text{ est irrationnelle}}$$

EXERCICE 39 : L'ÉQUATION DIOPHANTIENNE $ax + by = c$ ⋆⋆⋆⋆

a) Si $(x\,;y) \in E$, δ divise a et b, donc $ax + by = c$. Réciproquement, si $\delta \mid c$, écrivons $c = \delta c'$. L'identité de Bézout fournit u, v tels que $au + bv = \delta$, d'où $a(uc') + b(vc') = c$: le couple $(uc'\,;vc')$ est dans E.

$$\boxed{E \neq \varnothing \iff \delta \mid c}$$

b) Comme $ax_0 + by_0 = c$:

$$(x,y) \in E \iff ax + by = ax_0 + by_0 \iff a(x - x_0) = b(y_0 - y) \iff \delta a'(x - x_0) = \delta b'(y_0 - y)$$

et l'on simplifie par $\delta \neq 0$: $(x,y) \in E \iff a'(x - x_0) = b'(y_0 - y)$.

c) Si $(x\,;y) \in E$, b' divise $a'(x-x_0)$ et $\text{PGCD}(a',b') = 1$ (exercice 29, question 1), donc $b' \mid x - x_0$ d'après le théorème de Gauss : $x = x_0 + tb'$ avec $t \in \mathbb{Z}$. En reportant, $a'tb' = b'(y_0 - y)$, donc $y = y_0 - ta'$ puisque $b' \neq 0$. Réciproquement, pour $t \in \mathbb{Z}$, $a'(tb') = b'(ta')$, donc $(x_0 + tb'\,;y_0 - ta') \in E$ d'après b).

$$\boxed{E = \{(x_0 + tb'\,,\, y_0 - ta')\ ;\ t \in \mathbb{Z}\}}$$

Le piège est d'utiliser b et a au lieu de $b' = \frac{b}{\delta}$ et $a' = \frac{a}{\delta}$: on ne trouverait qu'une partie des solutions. On le voit à l'exercice 14, avec $33x + 45y = 12$ et $\delta = 3$: les solutions avancent de 15 et 11, et non de 45 et 33. L'exercice 19 en donne un autre exemple.

EXERCICE 40 ⋆⋆⋆⋆

Notons $D = \text{PGCD}(n^3 + n, 2n + 1)$, bien défini car $2n + 1 \neq 0$.

- D est premier avec n. Un diviseur commun de D et n divise $2n+1$ et n, donc $(2n+1) - 2n = 1$.
- D divise $n^2 + 1$. D divise $n^3 + n = n(n^2 + 1)$ et est premier avec n : d'après le théorème de Gauss, $D \mid n^2 + 1$.
- D divise 5. D divise $4(n^2+1)$ et $(2n-1)(2n+1) = 4n^2-1$, donc leur différence : $4n^2+4-4n^2+1 = 5$. Ainsi $D \in \{1\,;5\}$.
- Quand vaut-il 5 ? Si $D = 5$, alors $5 \mid 2n + 1$, soit $2n \equiv 4\ [5]$, d'où $n \equiv 2\ [5]$ en multipliant par 3, inverse de 2 modulo 5. Réciproquement, si $n \equiv 2\ [5]$, alors $2n+1 \equiv 5 \equiv 0$ et $n^3+n = n(n^2+1) \equiv 2 \times 5 \equiv 0\ [5]$, donc $5 \mid D$.

$$\boxed{\text{PGCD}(n^3 + n, 2n + 1) = \begin{cases} 5 & \text{si } n \equiv 2\ [5] \\ 1 & \text{sinon} \end{cases}}$$

Contrôle : $n = 2$ donne $\text{PGCD}(10, 5) = 5$; $n = 7$ donne $\text{PGCD}(350, 15) = 5$; $n = 3$ donne $\text{PGCD}(30, 7) = 1$. On reconnaît la méthode de l'exercice 11 : écarter le facteur n, premier avec $2n + 1$, puis éliminer n par une combinaison linéaire.

EXERCICE 41 ⋆⋆⋆⋆

Pour $k \in \mathbb{N}$, posons $N_k = a^k - 1$. On a $N_0 = 0$, et la suite (N_k) est strictement croissante car $a \geqslant 2$. L'exercice 31 du chapitre 1 établit que, si $n = mq + r$ avec $0 \leqslant r < m$, alors :

$$N_n = N_m \times Q + N_r \qquad \text{avec} \qquad 0 \leqslant N_r < N_m$$

pour un certain entier Q. Autrement dit, **le reste de la division de N_n par N_m est N_r, où r est le reste de la division de n par m.**

Supposons $n > m$, le cas $n = m$ étant immédiat et le cas $n < m$ s'y ramenant par symétrie. D'après la Proposition 2, $\text{PGCD}(N_n, N_m) = \text{PGCD}(N_m, N_r)$. Appliquons l'algorithme d'Euclide aux exposants : n, m, $r_0 = r$, r_1, …, jusqu'au dernier reste non nul $g = \text{PGCD}(m, n)$, suivi de 0. À chaque étape, les nombres N correspondants suivent exactement le même schéma :

$$\text{PGCD}(N_n, N_m) = \text{PGCD}(N_m, N_{r_0}) = \text{PGCD}(N_{r_0}, N_{r_1}) = \cdots$$

$$\cdots = \text{PGCD}(N_g, N_0) = \text{PGCD}(N_g, 0) = N_g$$

d'après la Proposition 1 pour la dernière égalité.

$$\boxed{\text{PGCD}\,(a^m - 1, a^n - 1) = a^{\text{PGCD}(m,n)} - 1}$$

On retrouve la question 3 de l'exercice 28 : $\text{PGCD}(4^{n+1} - 1, 4^n - 1) = 4^{\text{PGCD}(n+1,n)} - 1 = 4^1 - 1 = 3$. Autre exemple : $\text{PGCD}(2^{12} - 1, 2^{18} - 1) = 2^6 - 1 = 63$, ce que l'on vérifie avec $4095 = 63 \times 65$ et $262\,143 = 63 \times 4161$.

EXERCICE 42 : RELATION DE BÉZOUT À COEFFICIENTS DANS $\mathbb{N}$ ⋆⋆⋆⋆

a) Supposons par l'absurde que $ab - a - b = au + bv$ avec u et v dans $\mathbb{N}$. Alors :

$$ab = a(u+1) + b(v+1)$$

Ainsi a divise $ab - a(u+1) = b(v+1)$. Comme $\text{PGCD}(a,b) = 1$, le théorème de Gauss donne $a \mid v+1$; or $v+1 \geqslant 1$, donc $v+1 \geqslant a$. De même, $b \mid u+1$, donc $u+1 \geqslant b$. Mais alors :

$$ab = a(u+1) + b(v+1) \geqslant ab + ab = 2ab$$

ce qui est absurde puisque $ab > 0$. $\boxed{ab - a - b \text{ n'est pas de la forme } au + bv,\ (u,v) \in \mathbb{N}^2}$

b) Soit $n \geqslant ab - a - b + 1$. Pour $u \in \{0, \ldots, b-1\}$:

$$n - au \geqslant n - a(b-1) \geqslant ab - a - b + 1 - ab + a = 1 - b$$

Ces b entiers ont des restes distincts modulo b. En effet, si $n - au \equiv n - au'\ [b]$, alors $b \mid a(u'-u)$, donc $b \mid u'-u$ par le théorème de Gauss ; comme $|u'-u| < b$, on a $u = u'$. Les b restes possibles 0, 1, …, $b-1$ sont donc tous atteints, en particulier 0 : il existe $u_0 \in \{0, \ldots, b-1\}$ tel que $n - au_0 = bv_0$ avec $v_0 \in \mathbb{Z}$. Comme $bv_0 \geqslant 1 - b > -b$, on a $v_0 > -1$, donc $v_0 \in \mathbb{N}$.

$$\boxed{n = au_0 + bv_0 \text{ avec } (u_0, v_0) \in \mathbb{N}^2}$$

c) Avec $a = 5$ et $b = 8$, premiers entre eux, le plus grand montant impossible est :

$$\boxed{5 \times 8 - 5 - 8 = 27 \text{ centimes}}$$

et tout montant à partir de 28 centimes est payable. En testant les montants de 1 à 27, on trouve que les montants payables sont 5, 8, 10, 13, 15, 16, 18, 20, 21, 23, 24, 25 et 26. Les montants impossibles sont donc :

$$1,\ 2,\ 3,\ 4,\ 6,\ 7,\ 9,\ 11,\ 12,\ 14,\ 17,\ 19,\ 22,\ 27$$

Il y en a $14 = \dfrac{4 \times 7}{2} = \dfrac{(a-1)(b-1)}{2}$. Cette formule est générale : c'est la question c de l'exercice 507 du poly. On peut la contrôler sur $a = 3$, $b = 5$: les montants impossibles sont 1, 2, 4, 7, soit $4 = \frac{2 \times 4}{2}$, le plus grand valant $15 - 3 - 5 = 7$.