Exercice (2.9). *Algorithme d'Euclide et matrices* 2×2

Soient $a, b \in \mathbb{N}$, avec $a > b > 0$. On effectue l'algorithme d'Euclide : on pose $r_0 = a,\ r_1 = b$, et, supposant r_{j-1} et r_j construits, si $r_j \neq 0$ on note $r_{j-1} = r_j q_j + r_{j+1}$ la division euclidienne de r_{j-1} par r_j. On note n l'entier pour lequel l'algorithme s'arrête de sorte que $r_{n+1} = 0$ et r_n est le $PGCD$ de a, b.

1. Démontrer que $q_n \geqslant 2$.
2. a) Démontrer que, pour tout $k \in \{1, \ldots, n\}$, on a :
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} r_1 \\ r_0 \end{pmatrix}.$$
b) Démontrer qu'il existe deux suites de nombres entiers naturels $(a_k)_{1 \leqslant k \leqslant n+1}$ et $(b_k)_{1 \leqslant k \leqslant n+1}$ telles que, pour $k \in \{1, \ldots, n\}$,
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} = \begin{pmatrix} b_k & b_{k+1} \\ a_k & a_{k+1} \end{pmatrix}.$$
c) Démontrer que $b_1 = 0,\ b_2 = 1,\ a_1 = 1,\ a_2 = q_1$ et, pour $2 \leqslant j \leqslant n$, que $a_{j+1} = a_j q_j + a_{j-1}$ et $b_{j+1} = b_j q_j + b_{j-1}$. En déduire que les deux suites (a_k) et (b_k) sont croissantes et que $a_{n+1} \geqslant 2a_n$ et $b_{n+1} \geqslant 2b_n$. Dans quel cas a-t-on égalité dans l'une de ces inégalités ?
d) Pour $1 \leqslant k \leqslant n$, établir l'égalité $b_k a_{k+1} - b_{k+1} a_k = (-1)^k$.
e) Démontrer que l'on a une relation de Bézout
$$r_n = (-1)^n b_n a + (-1)^{n+1} a_n b.$$
3. a) Démontrer que $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^k = \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix}$, où F_k est le k-ème nombre de Fibonacci.
b) Démontrer que $a_k \geqslant F_k$ et $b_k \geqslant F_{k-1}$.
4. Expliquer en quoi cette méthode permet de trouver « rapidement » le $PGCD$ de a et b et une identité de Bézout $d = au + bv$.
5. On suppose que a et b sont premiers entre eux. Démontrer qu'il existe $n \in \mathbb{N}^*$ une suite $q_1, \ldots, q_n$ de nombres entiers strictement positifs et $u, v \in \mathbb{N}$ tels que $q_n \geqslant 2$ et
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} v & b \\ u & a \end{pmatrix}.$$

6. On suppose donnés $n \in \mathbb{N}^*$, une suite $(q_1, \dots, q_n)$ de nombres entiers strictement positifs, et $u, v \in \mathbb{N}$ tels que $q_n \geqslant 2$ et
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} v & b \\ u & a \end{pmatrix}.$$
Démontrer que les entiers a et b sont premiers entre eux et que la suite des quotients successifs de la division euclidienne de a par b est $q_1, q_2, \dots, q_n$.

1. Puisque $r_{n+1} = 0$, il vient $r_{n-1} = q_n r_n$; or, $r_n < r_{n-1}$ (c'est un reste de division euclidienne), donc $q_n > 1$; enfin $q_n \geqslant 2$ (car c'est un entier).

2. a) L'égalité $r_{k-1} = q_k r_k + r_{k+1}$ se lit :
$$(E_k) \qquad \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} r_k \\ r_{k-1} \end{pmatrix}.$$
On procède par récurrence sur k. Pour $k = 1, \dots, n$, notons (P_k) l'égalité
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} r_1 \\ r_0 \end{pmatrix}.$$
L'identité (E_1) donne P_1.
Si (P_{k-1}) est vrai, l'identité (E_k) donne (P_k).

b) Écrivons :
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} = \begin{pmatrix} b_k & d_k \\ a_k & c_k \end{pmatrix} = A_k.$$
L'égalité $\begin{pmatrix} b_k & d_k \\ a_k & c_k \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_{k+1} \end{pmatrix} = \begin{pmatrix} b_{k+1} & d_{k+1} \\ a_{k+1} & c_{k+1} \end{pmatrix}$ donne $a_{k+1} = c_k$ et $b_{k+1} = d_k$.

c) Et, pour $1 \leqslant k \leqslant n-1$, $a_{k+2} = c_{k+1} = a_{k+1} q_{k+1} + a_k \geqslant a_{k+1}$ et, de même $b_{k+2} = b_{k+1} q_{k+1} + b_k \geqslant b_{k+1}$.
Pour $k = 1$, on trouve $b_1 = 0,\ b_2 = 1,\ a_1 = 1,\ a_2 = q_1$.
Si $n = 1$ on a $b_{n+1} = 1 > 2b_1 = 0$ et $a_{n+1} = q_n \geqslant 2 = 2a_n$.
Sinon, $a_{n+1} = q_n a_n + a_{n-1} \geqslant 2a_n + a_1 > 2a_n$ et $b_{n+1} = q_n b_n + b_{n-1} \geqslant 2b_n$ avec égalité possible si $b_{n-1} = 0$ ce qui impose $n = 2$ (car sinon $b_{n-1} \geqslant b_2 = 1$) et $b_3 = 2$.

d) La matrice A_k est produit de k matrices de déterminant -1. Son déterminant est $(-1)^k$.

e) On a $A_n \begin{pmatrix} r_{n+1} \\ r_n \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}$ d'où $\begin{pmatrix} r_{n+1} \\ r_n \end{pmatrix} = A_n^{-1} \begin{pmatrix} b \\ a \end{pmatrix}$. La formule de la comatrice donne $A_n^{-1} = (-1)^n \begin{pmatrix} a_{n+1} & -b_{n+1} \\ -a_n & b_n \end{pmatrix}$, ([1]) d'où le résultat.

3. a) L'égalité se démontre par récurrence sur k ; elle est vraie pour $k = 1$ car $F_0 = 0$, $F_1 = F_2 = 1$; si elle est vraie pour k, on a

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{k+1} &= \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} F_k & F_{k-1} + F_k \\ F_{k+1} & F_k + F_{k+1} \end{pmatrix} \\ &= \begin{pmatrix} F_k & F_{k+1} \\ F_{k+1} & F_{k+2} \end{pmatrix}. \end{aligned}$$

b) Les inégalités $a_k \geqslant F_k$ et $b_k \geqslant F_{k-1}$ se démontrent par récurrence forte sur k. Elles sont vraies pour $k = 1$ et $k = 2$. Si elles ont vraies pour k et $k+1$, on a

$$a_{k+2} = q_{k+1} a_{k+1} + a_k \geqslant a_{k+1} + a_k \geqslant F_{k+1} + F_k = F_{k+2}$$

et

$$b_{k+2} = q_{k+1} b_{k+1} + b_k \geqslant b_{k+1} + b_k \geqslant F_k + F_{k-1} = F_{k+1}.$$

4. On construit des suites a_k, b_k, r_k ; il suffit de garder en mémoire uniquement deux termes consécutifs de ces trois suites pour construire le suivant. On s'arrête quand $r_{n+1} = 0$; on a alors le pgcd de a, b (c'est r_n) et une relation de Bézout grâce à la question 2.e). La question 3 nous indique que la convergence est assez rapide : s'il faut n divisions euclidiennes, on a $b = b_{n+1} r \geqslant F_n$: donc si $b < F_\ell$ il faut au plus $\ell - 1$ étapes. Or, F_ℓ croît géométriquement en ℓ.

5. Puisque a et b sont premiers entre eux, il existe n tel que $r_n = 1$ et $r_{n+1} = 0$. On a donc :

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}.$$

Cela donne :

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} v & b \\ u & a \end{pmatrix}.$$

[1] Plus généralement, on a la formule $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$, pour toute matrice 2×2 inversible.

6. Si l'on a une telle égalité, le calcul du déterminant nous donne une relation de Bézout $va - ub = (-1)^n$, donc a et b sont premiers entre eux. Démontrons par récurrence sur n que $b < a$ et que les quotients successifs de la division de a par b sont les q_j.

   Si $n = 1$, on a $b = 1$ et $a = q_1 \geqslant 2$.

   Supposons $n \geqslant 2$ et le cas de longueur $n-1$ traité. Écrivons :

$$\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_3 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} v' & b' \\ u' & a' \end{pmatrix}.$$

   D'après l'hypothèse de récurrence, $b' < a'$ et les quotients successifs de la division euclidienne de a' par b' sont $q_2, q_3, \ldots, q_n$. Or, $\begin{pmatrix} v & b \\ u & a \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} v' & b' \\ u' & a' \end{pmatrix}$, soit $a' = b$ et $a = q_1 b + b'$. Le quotient de a par b est donc q_1 et le reste b'. On en déduit que la suite des quotients successifs de la division euclidienne de b par a est bien $q_1, q_2, \ldots, q_n$.

Exercice (2.10). *Algorithme de Cornacchia* (*)

1. Soient $a, b \in \mathbb{N}$ tels que $b < a$ et $a^2 + b^2$ soit un nombre premier $p \neq 2$.
   a) Démontrer que a et b sont premiers entre eux.
   b) Démontrer qu'il existe $n \in \mathbb{N}^*$, des nombres entiers strictement positifs $q_1, \ldots, q_n$ avec $q_n \geqslant 2$ et des nombres $u, v \in \mathbb{N}$ tels que
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} v & b \\ u & a \end{pmatrix}.$$
   c) Démontrer que $2u \leqslant a$ et $2v \leqslant b$.
   d) Démontrer que $\begin{pmatrix} v & u \\ b & a \end{pmatrix} \begin{pmatrix} v & b \\ u & a \end{pmatrix} = \begin{pmatrix} x & \ell \\ \ell & p \end{pmatrix}$, où $x \in \mathbb{N}$ et ℓ est l'unique entier tel que $\ell^2 \equiv -1\ [p]$ et $0 < \ell < p/2$.
2. Soit $p > 2$ un nombre premier tel que -1 soit un carré modulo p (*i.e.* congru à 1 modulo 4 — voir exercice 2.21). Supposons que l'on ait trouvé ℓ tel que $0 < \ell < p/2$ et $\ell^2 = xp - 1$ avec $x \in \mathbb{N}$. Expliquer comment, grâce à l'algorithme d'Euclide, on trouve alors a et b tels que $a^2 + b^2 = p$.

1. a) Soit d le plus grand commun diviseur de a et b. Alors d^2 divise p, donc d divise p et $d \neq p$ soit $d = 1$.

   b) L'existence et unicité de $q_1, \ldots, q_n$ résultent de l'exercice 2.9.

c) On a $\begin{pmatrix} v & b \\ u & a \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix}$, où

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_{n-1} \end{pmatrix},$$

(avec $\alpha, \beta, \gamma, \delta \in \mathbb{N}$ — *cf.* exerc. 2.9). Il vient $v = \beta$, $u = \delta$, puis $b = q_n v + \alpha \geqslant 2v$ et $a = q_n u + \delta \geqslant 2u$ (puisque $q_n \geqslant 2$).

d) Écrivons $\begin{pmatrix} v & u \\ b & a \end{pmatrix} \begin{pmatrix} v & b \\ u & a \end{pmatrix} = \begin{pmatrix} x & \ell \\ k & p \end{pmatrix}$. Cette matrice est symétrique et donc $k = \ell$. On a $2\ell = 2(ua + bv) \leqslant p$ d'après la question précédente. Enfin le déterminant de cette matrice est 1 (c'est un produit pair de matrices de déterminant -1), donc $\ell^2 \equiv -1\ [p]$. Or, si -1 est un carré dans le corps $\mathbb{Z}/p\mathbb{Z}$, alors -1 a deux racines α et $-\alpha$. Une seule des deux a un représentant dans $[1, (p-1)/2]$.

2. D'après l'exercice 2.9, l'algorithme d'Euclide fournit un entier m non nul, un m-uplet $(q_1, \ldots, q_m)$ d'entiers $\geqslant 1$ avec $q_m \geqslant 2$ et $\alpha, \beta \in \mathbb{N}$ tels que $\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_m \end{pmatrix} = \begin{pmatrix} \alpha & \ell \\ \beta & p \end{pmatrix}$ et l'on a $\beta \leqslant p/2$.
Prenant les déterminants, il vient $-\beta\ell \equiv (-1)^m\ [p]$, donc la classe modulo p de β est, au signe près l'inverse de celle ℓ, c'est-à-dire celle de $\pm\ell$; puisque $0 \leqslant \beta < p/2$, il vient $\beta = \ell$ et m est pair. Prenant les transposées, on trouve :

$$\begin{pmatrix} 0 & 1 \\ 1 & q_m \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_{m-1} \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} = \begin{pmatrix} \alpha & \ell \\ \ell & p \end{pmatrix},$$

et par unicité, on trouve $q_j = q_{m+1-j}$.
Posons $m = 2k$ et

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} = \begin{pmatrix} v & u \\ b & a \end{pmatrix} = A.$$

On a $\begin{pmatrix} \alpha & \ell \\ \ell & p \end{pmatrix} = A^t A$, donc $p = a^2 + b^2$.

De l'égalité $A \begin{pmatrix} v & b \\ u & a \end{pmatrix} = \begin{pmatrix} \alpha & \ell \\ \ell & p \end{pmatrix}$, on déduit $A \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} \ell \\ p \end{pmatrix}$.
D'après l'exercice 2.9, on a :

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} \ell \\ p \end{pmatrix}.$$

Or, la matrice A est inversible, donc $a = r_k$ et $b = r_{k+1}$. Notons aussi que $r_{k-1} \geqslant r_k + r_{k+1}$, donc $r_{k-1}^2 > p$. En d'autres termes, a et b sont les deux premiers restes inférieurs à $\sqrt{p}$ dans les divisions euclidiennes successives entre p et ℓ.

Exercice (2.11). *Jouons avec la suite de Fibonacci*

1. Écrire les premiers nombres de Fibonacci. Lesquels sont pairs ? multiples de 3 ? multiples de 5 ?
2. a) Démontrer que, si m divise n, alors F_m divise F_n.
   b) Démontrer que, pour tout n, l'ensemble des $k \in \mathbb{N}$ tels que n divise F_k est de la forme $a\mathbb{N}$, où $a \in \mathbb{N}^*$.

   Soit $p \geqslant 7$ un nombre premier. Notons J la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ à coefficients dans $\mathbb{F}_p$.
3. On suppose que 5 est un carré modulo p. Démontrer que la matrice J est diagonalisable (dans $\mathbb{F}_p$). En déduire que F_{p-1} est multiple de p.
4. (*) On suppose que 5 n'est pas un carré modulo p.
   Notons $K = \{aI_2 + bJ\,;\ a, b \in \mathbb{F}_p\}$. Démontrer ce qui suit :
   a) l'ensemble K est un sous-anneau commutatif de $M_2(\mathbb{F}_p)$;
   b) l'anneau K est un corps commutatif ;
   c) l'application $x \mapsto x^p$ est un automorphisme involutif de K ;
   d) pour $x \in K$ on a $x^p = x \Leftrightarrow x \in \{aI_2;\ a \in \mathbb{F}_p\}$;
   e) posant $J' = J^p$, on a $J' \neq J$ et $J'^2 = J' + 1$;
   f) on a $J^p = -J^{-1}$;
   g) l'entier premier p divise F_{p+1} ; de plus, $F_p \equiv F_{p+2} \equiv -1 \ \ [p]$.

1. Les premiers nombres de Fibonacci sont les suivants.

n	0	1	2	3	4	5	6	7	8	9
F_n	0	1	1	2	3	5	8	13	21	34
n	10	11	12	13	14	15	16	17	18	19
F_n	55	89	144	233	377	610	987	1597	2584	4181

   D'après ce tableau, les F_{3k} sont pairs, les F_{4k} sont multiples de 3 et les F_{5k} sont multiples de 5…

2. a) Démontrons que $F_m | F_{km}$ par récurrence sur k.
   C'est vrai pour $k = 0$ (car $F_0 = 0$) et $k = 1$.

   On a $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^p = \begin{pmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{pmatrix}$; donc, pour tout $p, q \in \mathbb{N}$,

   $$\begin{pmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{pmatrix} \begin{pmatrix} F_{q-1} & F_q \\ F_q & F_{q+1} \end{pmatrix} = \begin{pmatrix} F_{p+q-1} & F_{p+q} \\ F_{p+q} & F_{p+q+1} \end{pmatrix}.$$

   Il vient $F_{p+q} = F_p F_{q-1} + F_{p+1} F_q$. On en déduit que, si F_p et F_q sont des multiples de F_m, il en va de même pour F_{p+q}. En particulier, si $F_m | F_{km}$, alors $F_m | F_{(k+1)m}$.

b) Pour $n \in \mathbb{N}$, notons $M_2(\mathbb{Z}/n\mathbb{Z})$ l'anneau des matrices 2×2 à coefficients dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ et $G_n = GL(2, \mathbb{Z}/n\mathbb{Z})$ le groupe formé par les éléments inversibles de cet anneau, c'est-à-dire les matrices 2×2 à coefficients dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ et inversibles. Notons aussi Δ_n le sous-groupe de G_n formé des matrices diagonales.
L'application $\psi : \mathbb{Z} \to G_n$ qui à $k \in \mathbb{Z}$ associe la classe dans le groupe $GL(2, \mathbb{Z}/n\mathbb{Z})$ de la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^k$ est un homomorphisme de groupes. Pour $k \in \mathbb{N}$, on a : $n | F_k \Leftrightarrow \psi(k) \in \Delta_n$. En d'autres termes, on a

$$\{k \in \mathbb{N} \,;\; n | F_k\} = \mathbb{N} \cap \psi^{-1}(\Delta_n).$$

Comme Δ_n est un sous-groupe de G_n et ψ est un homomorphisme de groupes, $\psi^{-1}(\Delta_n)$ est un sous-groupe de $\mathbb{Z}$; il existe un unique élément $a \in \mathbb{N}$ tel que $\psi^{-1}(\Delta_n) = a\mathbb{Z}$, donc $\mathbb{N} \cap \psi^{-1}(\Delta_n) = a\mathbb{N}$. Enfin, puisque G_n est fini, ψ n'est pas injective ; son noyau n'est pas réduit à $\{0\}$ et est contenu dans $\psi^{-1}(\Delta_n)$, donc $a \neq 0$.

Soit $p \geqslant 7$ un nombre premier. Remarquons que $X^2 - X - 1$ admet une racine dans $\mathbb{F}_p$ si et seulement si 5 (le discriminant de ce trinôme) est un carré dans $\mathbb{F}_p$. En voici la preuve.

- Supposons qu'il existe $a \in \mathbb{F}_p$ tel que $a^2 = 5$. Comme $5 \neq 0$, il vient $a \neq 0$. De plus, $p \neq 2$, donc 2 est inversible dans $\mathbb{F}_p$. Alors, les deux éléments $\alpha = \dfrac{1+a}{2}$ et $\beta = \dfrac{1-a}{2}$ sont racines distinctes du polynôme de degré 2 donné par $X^2 - X - 1$ sur $\mathbb{F}_p$.
- Supposons que $\alpha \in \mathbb{F}_p$ est racine du polynôme $X^2 - X - 1$; d'où, $\alpha^2 = \alpha + 1$, donc $(2\alpha - 1)^2 = 4\alpha^2 - 4\alpha + 1 = 4(\alpha + 1) - 4\alpha + 1 = 5$.

3. On suppose que 5 est un carré modulo p. Alors, le polynôme caractéristique $X^2 - X - 1$ de J a deux racines distinctes α, β, donc J est diagonalisable. Il existe donc $P \in GL(2, \mathbb{F}_p)$ tel que $PJP^{-1} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$.
Par le petit théorème de Fermat on a $\alpha^{p-1} = \beta^{p-1} = 1$ (notons que α et β sont non nuls car J est inversible — son déterminant est -1). On a donc $J^{p-1} = P^{-1} \begin{pmatrix} \alpha^{p-1} & 0 \\ 0 & \beta^{p-1} \end{pmatrix} P = I_2$. La classe modulo p de $\begin{pmatrix} F_{p-2} & F_{p-1} \\ F_{p-1} & F_p \end{pmatrix}$ est donc I_2, et p divise F_{p-1}.

4. a) L'ensemble K est un sous-espace vectoriel, donc un sous-groupe additif de $M_2(\mathbb{F}_p)$. Comme $J^2 = J + I_2$, pour $a, b, c, d \in \mathbb{F}_p$, on a :

$$\begin{aligned}(aI_2 + bJ)(cI_2 + dJ) &= acI_2 + (ad + bc)J + bd(J + I_2) \\ &= (ac + bd)I_2 + (ad + bc + bd)J,\end{aligned}$$