DM 6. Corrigé

Problème 1

1) Soit $x, y \in E$. L'ordre étant total, $x \preceq y$ ou bien $y \preceq x$, donc $\neg(x \prec y) \Longleftrightarrow x \succeq y$.
Ainsi, $x \ T \ y \Longleftrightarrow (x \succeq y) \wedge (x \preceq y) \Longleftrightarrow x = y$.
Ainsi, lorsque l'ordre est total, la relation T est la relation d'égalité.

2)
2.a) Soit $x \in E$. la propriété $(x \prec x)$ est fausse, donc $x \ T \ x$. Ainsi, T est réflexive.
Soit $x, y \in E$ tels que $x \ T \ y$. Ainsi $(\neg(x \prec y) \wedge \neg(y \prec x))$, donc $(\neg(y \prec x) \wedge \neg(x \prec y))$ et $y \ T \ x$. Ainsi T est symétrique.
2.b) 2 et 3 sont distincts et ne sont pas comparables pour la relation de divisibilité, donc on a bien $\neg((2|3) \wedge (2 \neq 3)) \ \wedge \ \neg((3|2) \wedge (2 \neq 3))$. Ainsi, $2 \ T \ 3$. De même, on montre que $3 \ T \ 4$. Si T était une relation d'équivalence, par transitivité, on pourrait en déduire que $2 \ T \ 4$, ce qui est faux car $(2|4) \wedge (2 \neq 4)$. Ainsi, dans ce cas, T n'est pas une relation d'équivalence.

3) Soit $x, y \in E$. Supposons que $x^- = y^-$.
$x \notin x^-$, donc $y \notin x^-$, puis $\neg(y \prec x)$.
Par symétrie des rôles joués par x et y, on a aussi $\neg(x \prec y)$, donc $x \ T \ y$.

4) Soit $x, y, z \in E$ tels que $x \ T \ y \ T \ z$. Alors $x^- = y^- = z^-$, donc $x^- = z^-$, donc d'après la question précédente, $x \ T \ z$. Ainsi T est transitive, donc d'après la question 2.a, T est une relation d'équivalence.

5) On suppose que T est une relation d'équivalence.
Soit $x, y \in E$ tel que $x \ T \ y$. Ainsi, $\neg(x \prec y)$ et $\neg(y \prec x)$.
Soit $z \in x^-$ (ainsi $z \prec x$). On souhaite montrer que $z \in y^-$. Raisonnons par l'absurde en supposant que $z \notin y^-$.
Ainsi, $\neg(z \prec y)$. De plus, si $y \prec z$, sachant que $z \prec x$, on en déduit que $y \prec x$, ce qui est faux. Ainsi, $\neg(y \prec z)$, donc $y \ T \ z$, or $x \ T \ y$ et T est une relation d'équivalence, donc par transitivité, $x \ T \ z$. En particulier, $\neg(z \prec x)$, ce qui est faux.
Cette contradiction montre que $z \in y^-$, lorsque $z \in x^-$, donc $x^- \subset y^-$.
De plus, on a aussi $y \ T \ x$, donc en remplaçant le couple (x, y) par le couple (y, x), on déduit du point précédent que $y^- \subset x^-$.
Ainsi, $x^- = y^-$.

Problème 2

1.a) D'après la propriété 1, $\emptyset \in \mathcal{C}$, donc d'après la propriété 2, $\Omega = \overline{\emptyset} \in \mathcal{C}$.
1.b) Soit $A, B \in \mathcal{C}$. D'après le cours, $A \cap B = \overline{\overline{A} \cup \overline{B}}$, donc $A \cap B \in \mathcal{C}$, d'après les propriétes 2 et 3.

2) Tout clan contient, d'après la question 1.a, $\{\emptyset, \Omega\}$, or ce dernier ensemble vérifie les propriétés 1, 2 et 3, donc c'est le plus petit clan sur Ω.

Tout clan sur Ω est par définition inclus dans $\mathcal{P}(\Omega)$, or ce dernier ensemble vérifie les propriétés 1, 2 et 3, donc c'est le plus grand clan sur Ω.

3) 1. $\emptyset =]0, 0[$, donc $\emptyset$ est un intervalle. Ainsi, $\emptyset$ est bien un élément de $\mathcal{I}$.
3. Si $A, B \in \mathcal{I}$, A et B sont deux réunions d'un nombre fini d'intervalles, donc $A \cup B$ est aussi une réunion d'un nombre fini d'intervalles, donc $A \cup B \in \mathcal{I}$.
2. Le complémentaire de l'intervalle $]a, +\infty[$ est l'intervalle $]-\infty, a]$, le complémentaire de l'intervalle $]a, b]$ (où $a \leq b$) est $]-\infty, a] \cup]b, +\infty[$. En examinant tous les cas possibles, on vérifie que le complémentaire d'un intervalle est toujours la réunion de 2 intervalles éventuellement vides.

Soit $A \in \mathcal{I}$. Il existe un nombre fini d'intervalles $I_1, \ldots, I_n$ tels que $A = \bigcup_{j=1}^{n} I_j$. Alors $\overline{A} = \bigcap_{j=1}^{n} \overline{I_j}$.
On vient de voir que, pour tout $j \in \{1, \ldots, n\}$, il existe deux intervalles $K_{j,1}, K_{j,2}$ tels que $\overline{I_j} = K_{j,1} \cup K_{j,2}$.
Ainsi, $\overline{A} = \bigcap_{j=1}^{n} (K_{j,1} \cup K_{j,2})$.
Par distributivité de l'intersection par rapport à la réunion, on en déduit que $\overline{A}$ est une réunion finie d'intersections d'intervalles, donc d'après l'énoncé, que c'est une réunion finie d'intervalles. Démontrons précisément que $\overline{A}$ est une réunion d'un nombre fini d'intervalles par récurrence sur n. On note $R(n)$ l'assertion suivante :

pour toutes familles d'intervalles $(K_{j,1})_{1 \leq j \leq n}$ et $(K_{j,2})_{1 \leq j \leq n}$, $\bigcap_{j=1}^{n} (K_{j,1} \cup K_{j,2})$ est une réunion finie d'intervalles.
Pour $n = 1$, $R(1)$ est claire.
Pour $n \geq 2$, supposons $R(n-1)$ et démontrons $R(n)$.
Soit $(K_{j,1})_{1 \leq j \leq n}$ et $(K_{j,2})_{1 \leq j \leq n}$ deux familles de n intervalles de $\mathbb{R}$.
Posons $E = \bigcap_{j=1}^{n} (K_{j,1} \cup K_{j_2})$.
$E = (K_{n,1} \cup K_{n,2}) \cap \left(\bigcap_{j=1}^{n-1} (K_{j,1} \cup K_{j,2}) \right)$. Par hypothèse de récurrence, il existe un nombre

fini d'intervalles $I_1, \ldots, I_k$ tels que $\displaystyle\bigcap_{j=1}^{n-1}(K_{j,1} \cup K_{j,2}) = \bigcup_{h=1}^{k} I_h$,

donc $E = (K_{n,1} \cup K_{n,2}) \cap \Big(\displaystyle\bigcup_{h=1}^{k} I_h\Big)$. D'après la distributivité de l'intersection par rapport à la réunion, on a vu dans le cours que $E = \Big(K_{n,1} \cap \Big(\displaystyle\bigcup_{h=1}^{k} I_h\Big)\Big) \cup \Big(K_{n,2} \cap \Big(\displaystyle\bigcup_{h=1}^{k} I_h\Big)\Big)$.
Toujours d'après la distributivité de l'intersection par rapport à la réunion,
$E = \Big(\displaystyle\bigcup_{h=1}^{k}(K_{n,1} \cap I_h)\Big) \cup \Big(\displaystyle\bigcup_{h=1}^{k}(K_{n,2} \cap I_h)\Big)$.
D'après l'énoncé, l'intersection de 2 intervalles est toujours un intervalle, donc E est bien une réunion d'un nombre fini d'intervalles. Ceci prouve $R(n+1)$.
D'après le principe de récurrence, $R(n)$ est vrai pour tout $n \in \mathbb{N}^*$, ce qui résout cette question.

4) 1. Avec $I = \emptyset$, $\displaystyle\bigcup_{i \in I} E_i = \emptyset$, donc $\emptyset \in \mathcal{C}$.

3. Soit $A, B \in \mathcal{C}$. Il existe $I, J \subset \{1, \ldots, n\}$ tels que $A = \displaystyle\bigcup_{i \in I} E_i$ et $B = \displaystyle\bigcup_{i \in F} E_i$. Alors, par associativité de la réunion, $A \cup B = \displaystyle\bigcup_{i \in I \cup J} E_i$. Donc $A \cup B \in \mathcal{C}$.

2. Soit $A \in \mathcal{C}$. Il existe $I \subset \{1, \ldots, n\}$ tel que $A = \displaystyle\bigcup_{i \in I} E_i$.

$(E_1, \ldots, E_n)$ étant une partition de Ω, Ω est l'union disjointe suivante :
$\Omega = \Big(\displaystyle\bigcup_{i \in I} E_i\Big) \sqcup \Big(\displaystyle\bigcup_{i \in \overline{I}} E_i\Big)$, où $\overline{I}$ désigne le complémentaire de I dans $\{1, \ldots, n\}$.
En effet, si $x \in \Big(\displaystyle\bigcup_{i \in I} E_i\Big) \cap \Big(\displaystyle\bigcup_{i \in \overline{I}} E_i\Big)$, il existe $i \in I$ et $j \in \overline{I}$ tels que $x \in E_i \cap E_j = \emptyset$, ce qui est impossible.
Ainsi, $\overline{A} = \displaystyle\bigcup_{i \in \overline{I}} E_i \in \mathcal{C}$.

5.a) On a bien sûr $(x \in A) \Longleftrightarrow (x \in A)$, donc pour tout $x \in \Omega$, $x\ R\ x$, ce qui prouve que R est réflexive.
Soit $x, y \in \Omega$ tels que $x\ R\ y$. Alors, pour tout $A \in \mathcal{C}$, $(y \in A) \Longleftrightarrow (x \in A)$, donc $y\ R\ x$, ce qui prouve que R est symétrique.
Soit $x, y, z \in \Omega$ tels que $x\ R\ y\ R\ z$. Pour tout $A \in \mathcal{C}$, $(x \in A) \Longleftrightarrow (y \in A) \Longleftrightarrow (z \in A)$, donc d'après le modus ponens, $x\ R\ z$.
Ceci prouve que R est transitive, donc R est une relation d'équivalence sur Ω.
5.b) Soit $A \in \mathcal{C}$.
Pour tout $y \in A$, $y \in \hat{y}$, donc $y \in \displaystyle\bigcup_{x \in A} \hat{x}$. Ainsi, $A \subset \displaystyle\bigcup_{x \in A} \hat{x}$.
Soit $x \in A$. Soit $y \in \hat{x}$. Alors $x\ R\ y$, or $x \in A$, donc $y \in A$.

Ainsi, $\hat{x} \subset A$, puis $\bigcup_{x\in A} \hat{x} \subset A$.
On a ainsi prouvé que $A = \bigcup_{x\in A} \hat{x}$.
5.c) Notons que $\Omega \in \mathcal{C}$ et $x \in \Omega$, donc $\Omega \in \mathcal{C}_x$. Ainsi, $\mathcal{C}_x$ n'est pas vide et l'intersection $\bigcap_{X\in \mathcal{C}_x} X$ est bien définie.
Soit $y \in \hat{x}$. Soit $X \in \mathcal{C}_x$. $x\ R\ y$, donc pour tout $A \in \mathcal{C}$, $(x \in A) \Longleftrightarrow (y \in A)$, or $X \in \mathcal{C}$ et $x \in X$, donc $y \in X$.
Ainsi, $y \in \bigcap_{X\in \mathcal{C}_x} X$, pour tout $y \in \hat{x}$, donc $\hat{x} \subset \bigcap_{X\in \mathcal{C}_x} X$.
Réciproquement, soit $y \in \bigcap_{X\in \mathcal{C}_x} X$. Alors, pour tout $X \in \mathcal{C}$ tel que $x \in X$, on a $y \in X$.
Donc pour tout $A \in \mathcal{C}$, $(x \in A) \Longrightarrow (y \in A)$.
Soit $A \in \mathcal{C}$. $\mathcal{C}$ étant un clan, $\overline{A} \in C$, donc on a encore $(x \in \overline{A}) \Longrightarrow (y \in \overline{A})$. La contraposée de cette implication est également vraie, donc $(y \in A) \Longrightarrow (x \in A)$.
On a ainsi montré que, pour tout $A \in \mathcal{C}$, $(x \in A) \Longleftrightarrow (y \in A)$, donc que $x\ R\ y$.
Ainsi, pour tout $y \in \bigcap_{X\in \mathcal{C}_x} X$, $y \in \hat{x}$. Ceci montre la seconde inclusion $\bigcap_{X\in \mathcal{C}_x} X \subset \hat{x}$, ce qui résout la question.
5.d) Soit $x \in \Omega$. $\mathcal{C}_x \subset \mathcal{C}$, donc $\mathcal{C}_x$ est fini, or $\hat{x} = \bigcap_{X\in \mathcal{C}_x} X$, donc $\hat{x}$ est une intersection d'un nombre fini d'éléments de $\mathcal{C}$. Or d'après la question 1.b, une intersection de deux éléments de $\mathcal{C}$ est un élément de $\mathcal{C}$. Par récurrence, on montrerait qu'une intersection de n éléments de $\mathcal{C}$ est un élément de $\mathcal{C}$, pour tout $n \in \mathbb{N}^*$, donc $\hat{x} \in \mathcal{C}$.

$\mathcal{C}$ étant fini, ceci implique que R ne possède qu'un nombre fini de classes d'équivalence notées $E_1, \ldots, E_n$. D'après le cours, ces classes d'équivalence constituent une partition de Ω. Notons $\mathcal{C}'$ le clan engendré par cette partition.
Les éléments de $\mathcal{C}'$ sont des réunions finies de classes d'équivalence, mais on a vu que chaque classe d'équivalence est un élément de $\mathcal{C}$, or $\mathcal{C}$ est un clan, donc d'après la propriété 3, tout élément de $\mathcal{C}'$ est un élément de $\mathcal{C}$.
La réciproque se déduit immédiatement de la question 5.b, donc $\mathcal{C} = \mathcal{C}'$ est bien un clan engendré par une partition finie de Ω.

1 Coefficients optimaux de Bezout

1.1 Algorithme d'Euclide

1°) Par définition de la division euclidienne dans $\mathbb{Z}$, tant que $a_i \neq 0$, $0 \leq a_{i+1} < a_i$. Or l'ordre naturel sur les entiers est un bon ordre, donc il n'existe pas de suite infinie d'entiers naturels strictement décroissante. Ainsi, il existe nécessairement $N \in \mathbb{N}^*$ tel que $a_{N+1} = 0$.

2°) $\diamond$ **Lemme d'Euclide :** Soient $(a', b') \in \mathbb{N}^2$ avec $b' \neq 0$. Notons q et r les quotient et reste de la division euclidienne de a' par b'. Alors $a' \wedge b' = b' \wedge r$.
En effet, $a' = b'q + r$, donc si d est un diviseur commun de a' et b', alors d divise $a' - b'q = r$ et réciproquement, si d est un diviseur commun de b' et r, alors d divise $b'q + r = a'$. Or le PGCD de a' et b' est d'après le cours la borne inférieure pour la relation d'ordre de divisibilité de l'ensemble des diviseurs positifs communs de a' et b', donc c'est aussi le PGCD de b' et r.
$\diamond$ On notera $a' \wedge b'$ le PGCD de deux entiers relatifs a' et b'.
On déduit du lemme d'Euclide que, pour tout $i \in \mathbb{N}^*$, $a_{i-1} \wedge a_i = a_i \wedge a_{i+1}$, donc la suite $(a_i \wedge a_{i+1})_{0 \leq i \leq N}$ est constante. En particulier, $a \wedge b = a_N \wedge a_{N+1}$. Or d'après le cours, $a_N \wedge a_{N+1}$ est l'unique entier naturel n tel que $n\mathbb{Z} = a_N\mathbb{Z} + a_{N+1}\mathbb{Z}$. Ici $a_{N+1} = 0$, donc $n\mathbb{Z} = a_N\mathbb{Z}$ puis $n = a_N$. En conclusion $a \wedge b = a_N$.

3°) Pour $i \in \{0, \ldots, N-1\}$, notons $R(i)$ l'assertion : $\alpha_i a_i + \beta_i a_{i+1} = a \wedge b$. Montrons $R(i)$ pour tout $i \in \{0, \ldots, N-1\}$ par récurrence finie descendante.
Pour $i = N-1$, $\alpha_i a_i + \beta_i a_{i+1} = a_N = a \wedge b$, d'où $R(N-1)$.
Pour $i \in \{1, \ldots, N-1\}$, supposons $R(i)$. Ainsi, $\alpha_i a_i + \beta_i a_{i+1} = a \wedge b$, or $a_{i-1} = a_i q_i + a_{i+1}$, donc $a \wedge b = \alpha_i a_i + \beta_i(a_{i-1} - a_i q_i) = \beta_i a_{i-1} + (\alpha_i - \beta_i q_i)a_i$. Ainsi, en posant $\alpha_{i-1} = \beta_i$ et $\beta_{i-1} = \alpha_i - \beta_i q_i$, on obtient $a \wedge b = \alpha_{i-1} a_{i-1} + \beta_{i-1} a_i$, c'est-à-dire $R(i)$.
D'après le principe de récurrence,
pour tout pour tout $i \in \{0, \ldots, N-1\}$, $\alpha_i a_i + \beta_i a_{i+1} = a \wedge b$.
En particulier, pour $i = 0$, $\alpha_0 a + \beta_0 b = a \wedge b$.

1.2 Application

4°) Lorsqu'on applique l'algorithme d'Euclide avec $a = 67$ et $b = 35$, les divisions euclidiennes successives s'écrivent :

— $67 = 35 + 32$;
— $35 = 32 + 3$;
— $32 = 3 \times 10 + 2$;
— $3 = 2 + 1$;
— $2 = 2 \times 1 + 0$.

Ainsi, avec les notations de la première partie, $N = 5$ et $67 \wedge 35 = a_N = 1$, donc 67 et 35 sont premiers entre eux.

De plus, le calcul des coefficients $(\alpha_i, \beta_i)_{0\leq i\leq 3}$, d'après la démonstration de la question 3, correspond à la succession suivante d'égalités :

$$\begin{aligned}
1 &= 3-2 \\
&= 3-(32-3\times 10) \\
&= -32+11\times 3 \\
&= -32+11\times(35-32) \\
&= 11\times 35-12\times 32 \\
&= 11\times 35-12\times(67-35) \\
&= -12\times 67+23\times 35,
\end{aligned}$$

donc en posant $\alpha=-12$ et $\beta=23$, on obtient $67\alpha+35\beta=1$.

5°) Notons S le nombre de sushis. On sait que $S\equiv 21[35]$ et $S\equiv 4[67]$.
Posons $S'=21\times\alpha\times 67+4\beta\times 35$. Ainsi, modulo 35, $S'\equiv 21\times\alpha\times 67+21\beta\times 35=21$ et modulo 67, $S'\equiv 4\times\alpha\times 67+4\beta\times 35=4$.
Alors $S-S'\in 35\mathbb{Z}\cap 67\mathbb{Z}=(35\vee 67)\mathbb{Z}=(35\times 67)\mathbb{Z}$, car 35 et 67 sont premiers entre eux. Ainsi, $S\equiv S'[35\times 67]$, c'est-à-dire, avec l'aide de la calculatrice :
$S\equiv -13664\equiv 406[2345]$.
Donc $S\in[500,5000]\cap(406+2345\mathbb{Z})=\{2751\}$. On en déduit que le client a commandé exactement 2751 sushis.

1.3 Optimalité

6°) L'existence de $u_0, v_0\in\mathbb{Z}$ tels que $u_0a+v_0b=1$ résulte immédiatement de l'identité de Bezout, ou bien de la question 3.
Soit $u,v\in\mathbb{Z}$. Notons (B) la condition : $ua+vb=1$.
En soustrayant la relation $u_0a+v_0b=1$, on obtient $(B)\Longleftrightarrow(u-u_0)a+(v-v_0)b=0$.
Supposons que (B) est vérifiée. Alors $(u-u_0)a=b(v_0-v)$, donc $b\mid(u-u_0)a$, or $a\wedge b=1$, donc d'après le théorème de Gauss, $b\mid(u-u_0)$. Ainsi, il existe $k\in\mathbb{Z}$ tel que $u=u_0+kb$. Dans ces conditions,
$(B)\Longleftrightarrow kab=b(v_0-v)\Longleftrightarrow v=v_0-ka$, car $b\neq 0$.
Ainsi, $(B)\Longleftrightarrow[\exists k\in\mathbb{Z},\ \ u=u_0+kb$ et $v=v_0-ka]$. En conclusion,
l'ensemble des couples $(u,v)\in\mathbb{Z}^2$ tels que $ua+vb=1$ est $\{(u_0+kb, v_0-ka)\ /\ k\in\mathbb{Z}\}$.

7°)
$\diamond$ *Existence :* Écrivons la division euclidienne de u_0 par b :
il existe $r,q\in\mathbb{Z}$ tels que $u_0=qb+r$ avec $0\leq r<b$.
On a $r=u_0-qb$, donc en posant $s=v_0+qa$, on construit un couple (r,s) vérifiant (B) avec $0\leq r<b$.
Si r et s étaient de même signe, on aurait $1=|ra+sb|=|r|a+|s|b$ (cas d'égalité de l'inégalité triangulaire), or $a\geq 2$ et $b\geq 2$, donc $r=s=0$, ce qui est faux. Ainsi s est négatif.
De plus, $(-s)b=ra-1<ra<ba$, donc $0\leq -s<a$.
Enfin, si $r=0$, alors $1=sb$ ce qui est impossible avec $b\geq 2$. Donc $r\neq 0$ et de même, $s\neq 0$. En conclusion, (r,s) vérifie $ar+bs=1$ avec $0<r<b$ et $-a<s<0$.

Ceci prouve l'existence.
◇ Unicité : Supposons qu'il existe $(r', s') \in \mathbb{Z}^2$ tel que $ar' + bs' = 1$ avec $0 < r' < b$ et $-a < s' < 0$.
En appliquant la question 6, dans laquelle on peut remplacer (u_0, v_0) par (r, s), il existe $k \in \mathbb{Z}$ tel que $r' = r + kb$ et $s' = s - ka$. En particulier, $r' \equiv r\ [b]$, or $r, r' \in \{1, \ldots, b-1\}$, donc $r = r'$. Alors $k = 0$, donc $s' = s$.
Ceci prouve l'unicité.
◇ La seconde propriété d'existence-unicité se déduit de la première en échangeant les rôles joués par a et b.

8°) Nous reprenons les notations de la première partie. Notons $S(i)$ l'assertion :
$|\alpha_i| < a_{i+1}$, $|\beta_i| < a_i$, α_i a même signe que $(-1)^{N-i}$ (au sens large) et β_i est de signe opposé.
Montrons $S(i)$, pour tout $i \in \{0, \ldots, N-1\}$, par récurrence descendante finie.
◇ Lorsque $i = N-1$, $\alpha_{N-1} = 0$ et $\beta_{N-1} = 1$, or $0 = a_{N+1} < a_N < a_{N-1}$, donc $\alpha_{N-1} < a_N$ et $\beta_{N-1} < a_{N-1}$. De plus, le signe de β_{N-1} est bien l'opposé de celui de $(-1)^{N-(N-1)} = -1$. donc $S(N-1)$ est vérifiée.
◇ Soit $i \in \{1, \ldots, N-1\}$ tel que $S(i)$.
On a $\alpha_{i-1} = \beta_i$, donc d'après $S(i)$, $|\alpha_{i-1}| < a_i$ et α_{i-1} a même signe que $(-1)^{N-(i-1)}$.
On a $\beta_{i-1} = \alpha_i - \beta_i q_i$, or α_i et $-\beta_i q_i$ sont de même signe,
donc $|\beta_{i-1}| = |\alpha_i| + q_i|\beta_i| < a_{i+1} + q_i a_i = a_{i-1}$ et β_{i-1} a même signe que α_i, donc est de signe opposé à $\beta_i = \alpha_{i-1}$.
On a bien prouvé $S(i-1)$.
◇ En particulier, $S(0)$ prouve que $|\alpha_0| < a_1 = b$ et $|\beta_0| < a_0 = a$.
Le même argument qu'en question 7 montre que $\alpha_0 \neq 0$ et $\beta_0 \neq 0$. D'après l'unicité de la question 7, (α_0, β_0) est donc l'un des couples (u, v) de la question précédente.
◇ Il s'agit du couple (u, v) tel que $u > 0$ si et seulement si $\alpha_0 > 0$, donc si et seulement si $(-1)^N$ est positif. Ainsi, l'algorithme proposé en question 3 fournit des coefficients (u, v) de Bezout optimaux, c'est-à-dire tels que $|u| < b$ et $|v| < a$. De plus, il s'agit de l'unique couple (u, v) avec $u > 0$ si et seulement si N est pair, où N est le nombre de divisions euclidiennes réalisées par l'algorithme d'Euclide.

1.4 Un second algorithme de calcul des coefficients de Bezout

9°) Pour tout $i \in \{0, \ldots, N+1\}$, notons $R(i)$ l'assertion : $u_i a + v_i b = a_i$.
◇ Pour $i = 0$, $u_0 a + v_0 b = a = a_0$ et pour $i = 1$, $u_1 a + v_1 b = b = a_1$, donc $R(0)$ et $R(1)$ sont vrais.
◇ Soit $i \in \{1, \ldots, N\}$. On suppose $R(i-1)$ et $R(i)$.
On a $u_i a + v_i b = a_i$ et $u_{i-1} a + v_{i-1} b = a_{i-1}$, or $a_{i+1} = a_{i-1} - q_i a_i$, donc
$a_{i+1} = (u_{i-1} a + v_{i-1} b) - q_i(u_i a + v_i b) = (u_{i-1} - q_i u_i)a + (v_{i-1} - q_i v_i)b = u_{i+1} a + v_{i+1} b$.
D'où $R(i+1)$.
◇ D'après le principe de récurrence double, pour tout $i \in \{0, \ldots, N+1\}$, $u_i a + v_i b = a_i$.

10°) Soit $i \in \{1, \ldots, N\}$.

$u_{i+1}v_i - u_iv_{i+1} = (u_{i-1} - q_iu_i)v_i - u_i(v_{i-1} - q_iv_i) = u_{i-1}v_i - u_iv_{i-1}$, donc la suite $(|u_{i+1}v_i - u_iv_{i+1}|)_{0\leq i\leq N}$ est constante, or son premier terme est égal à $|u_1v_0 - u_0v_1| = 1$, donc, pour tout $i \in \{0, \dots, N\}$, $|u_iv_{i+1} - u_{i+1}v_i| = 1$.
D'après l'identité de Bezout, on en déduit que u_i et v_i sont premiers entre eux, mais aussi que u_{i+1} et v_{i+1} sont premiers entre eux, pour tout $i \in \{0, \dots, N\}$. Cela permet de conclure.

11°)
$\diamond$ Pour tout $i \in \{0, \dots, N+1\}$, notons $R(i)$ l'assertion : au sens large, u_i est du signe de $(-1)^i$ et v_i est du signe opposé.
Pour $i = 0$ ou $i = 1$, on a clairement $R(0)$ et $R(1)$.
Soit $i \in \{1, \dots, N\}$ tel que $R(i)$ et $R(i-1)$.
Alors $u_{i+1} = u_{i-1} - q_iu_i$ est la somme de deux quantités du signe de $(-1)^{i+1}$, donc u_{i+1} a même signe que $(-1)^{i+1}$. De même, on montre que v_{i+1} est du signe opposé, ce qui prouve $R(i+1)$.
$\diamond$ Soit $i \in \{1, \dots, N\}$: $|u_{i+1}| = (-1)^{i+1}u_{i+1} = (-1)^{i-1}u_{i-1} + (-1)^iu_iq_i = |u_{i-1}| + |u_i|q_i$.
De plus, $a_{i+1} < a_{i-1}$, donc $q_i = \dfrac{a_{i-1} - a_{i+1}}{a_i} > 0$ et $q_i \in \mathbb{N}$, donc $q_i \geq 1$.
Ainsi $|u_{i+1}| \geq |u_{i-1}| + |u_i| \geq |u_i|$.
En particulier, $|u_N| \leq |u_{N+1}|$. De même, on montre que $|v_N| \leq |v_{N+1}|$.
$\diamond$ On a $u_{N+1}a + v_{N+1}b = a_{N+1} = 0$, donc $u_{N+1} \mid v_{N+1}b$, or $u_{N+1} \wedge v_{N+1} = 1$, donc d'après le théorème de Gauss, $u_{N+1} \mid b$, mais $b \neq 0$, donc $|u_{N+1}| \leq b$. De même, $|v_{N+1}| \leq a$.
$\diamond$ On en déduit que $|u_N| \leq b$ et $|v_N| \leq a$. De plus, $u_Na + v_Nb = a_N = 1$.
Si $|u_N| \in \{0, b\}$, alors $1 = u_Na + v_Nb \equiv 0$ $[b]$, ce qui est faux, donc $|u_N| \in \{1, \dots, b-1\}$ et de même, $|v_N| \in \{1, \dots, a-1\}$. De plus, u_N et v_N sont de signes opposés.
D'après l'unicité de la question 7, et d'après la question 8, pour montrer que $(\alpha_0, \beta_0) = (u_N, v_N)$, il suffit d'établir que α_0 et u_N ont le même signe. C'est le cas, car on a montré que α_0 et u_N ont tous les deux le même signe que $(-1)^N$.

En conclusion, à partir de l'algorithme d'Euclide, les questions 3 et 9 indiquent deux algorithmes différents pour construire des coefficients de Bezout u, v tels que $ua + vb = 1$. On a montré que ces deux algorithmes fournissent le même couple de coefficients de Bezout et que ce dernier satisfait la condition d'optimalité suivante : $|u| < b$ et $|v| < a$.