Calcul d'inverse dans $\mathbb{Z}/n\mathbb{Z}$

Comment inverser un élément de $\mathbb{Z}/n\mathbb{Z}$. Dans les exercices *Relations de Bézout dans* $\mathbb{Z}$ de *La Banque des Cent*, j'explique ma façon de remonter l'algorithme pour obtenir les coefficients de Bézout (avec plus de détails que dans ce corrigé). Mais avant de foncer à corps perdu dans l'algorithme, regardez si vous ne parvenez pas à trouver l'inverse « de tête », en voyant un multiple convenable de l'entier a à inverser modulo n, qui serait presque égal à un multiple de n (s'il diffère de 1, alors vous avez trouvé un entier b tel que : $ab \equiv 1 \bmod n$ et b est l'inverse cherché ; s'il diffère de -1, vous avez trouvé un entier b tel que $ab \equiv -1 \bmod n$, et dans ce cas $-b$ est l'inverse cherché).

Corrigé 1. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases} 16 &= 3\times 5+1 \\ 3 &= 1\times 3+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 16 et 3 est 1, c'est-à-dire : 3 est inversible modulo 16. De plus la première division euclidienne implique immédiatement : $16u+3v=1$, avec : $(u,v)=(1,-5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 16, et on a : $3v\equiv 1 \bmod 16$. Ceci prouve que 3 admet pour inverse modulo 16 : $v=-5$. D'où le résultat.

Corrigé 2. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases} 23 &= -4\times(-5)+3 & \left(\text{matriciellement : } \begin{pmatrix} 23 \\ -4 \end{pmatrix} = \begin{pmatrix} -5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -4 \\ 3 \end{pmatrix}\right) \\ -4 &= 3\times(-2)+2 & \left(\text{matriciellement : } \begin{pmatrix} -4 \\ 3 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}\right) \\ 3 &= 2\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 &= 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 23 et -4 est 1, c'est-à-dire : -4 est inversible modulo 23. Déduisons-en aussi des entiers u et v tels que : $23u+-4v=1$. Les relations matricielles ci-dessus impliquent :

$$1=\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 5 \end{pmatrix}\begin{pmatrix}23\\-4\end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & -6 \end{pmatrix}$$

En résumé on a : $1=\begin{pmatrix} -1 & -6 \end{pmatrix}\begin{pmatrix}23\\-4\end{pmatrix}$, c'est-à-dire : $23u-4v=1$, avec : $(u,v)=(-1,-6)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 23, et on a : $-4v\equiv 1 \bmod 23$. Ceci prouve que -4 admet pour inverse modulo 23 : $v=-6$. D'où le résultat.

Corrigé 3. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 1

$$\begin{cases} 301 &= -5\times(-60)+1 \\ -5 &= 1\times(-5)+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 301 et -5 est 1, c'est-à-dire : -5 est inversible modulo 301. De plus la première division euclidienne implique immédiatement : $301u-5v=1$, avec : $(u,v)=(1{,}60)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 301, et on a : $-5v\equiv 1 \bmod 301$. Ceci prouve que -5 admet pour inverse modulo 301 : $v=60$. D'où le résultat.

Corrigé 4. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu ← page 1

la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 46 &= -9 \times (-5) + 1 \\ -9 &= 1 \times (-9) + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 46 et -9 est 1, c'est-à-dire : -9 est inversible modulo 46. De plus la première division euclidienne implique immédiatement : $46u - 9v = 1$, avec : $(u, v) = (1{,}5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 46, et on a : $-9v \equiv 1 \bmod 46$. Ceci prouve que -9 admet pour inverse modulo 46 : $v = 5$. D'où le résultat.

Corrigé 5. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases} 22 &= -9 \times (-2) + 4 & \left(\text{matriciellement :} \quad \begin{pmatrix} 22 \\ -9 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -9 \\ 4 \end{pmatrix} \right) \\ -9 &= 4 \times (-3) + 3 & \left(\text{matriciellement :} \quad \begin{pmatrix} -9 \\ 4 \end{pmatrix} = \begin{pmatrix} -3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 \\ 3 \end{pmatrix} \right) \\ 4 &= 3 \times 1 + 1 & \left(\text{matriciellement :} \quad \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} \right) \\ 3 &= 1 \times 3 + 0 & \left(\text{matriciellement :} \quad \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 22 et -9 est 1, c'est-à-dire : -9 est inversible modulo 22. Déduisons-en aussi des entiers u et v tels que : $22u + -9v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 22 \\ -9 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & -2 \end{pmatrix} \to \begin{pmatrix} -2 & -5 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -2 & -5 \end{pmatrix} \begin{pmatrix} 22 \\ -9 \end{pmatrix}$, c'est-à-dire : $22u - 9v = 1$, avec : $(u, v) = (-2, -5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 22, et on a : $-9v \equiv 1 \bmod 22$. Ceci prouve que -9 admet pour inverse modulo 22 : $v = -5$. D'où le résultat.

Corrigé 6. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases} 17 &= -5 \times (-3) + 2 & \left(\text{matriciellement :} \quad \begin{pmatrix} 17 \\ -5 \end{pmatrix} = \begin{pmatrix} -3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -5 \\ 2 \end{pmatrix} \right) \\ -5 &= 2 \times (-3) + 1 & \left(\text{matriciellement :} \quad \begin{pmatrix} -5 \\ 2 \end{pmatrix} = \begin{pmatrix} -3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right) \\ 2 &= 1 \times 2 + 0 & \left(\text{matriciellement :} \quad \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 17 et -5 est 1, c'est-à-dire : -5 est inversible modulo 17. Déduisons-en aussi des entiers u et v tels que : $17u + -5v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 3\end{pmatrix}\begin{pmatrix}17\\ -5\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & 3\end{pmatrix} \to \begin{pmatrix}3 & 10\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}3 & 10\end{pmatrix}\begin{pmatrix}17\\ -5\end{pmatrix}$, c'est-à-dire : $17u - 5v = 1$, avec : $(u, v) = (3{,}10)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 17, et on a : $-5v \equiv 1 \bmod 17$. Ceci prouve que -5 admet pour inverse modulo 17 : $v = 10$. D'où le résultat.

Corrigé 7. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 1

$$\begin{cases} 67 = 4 \times 16 + 3 & \left(\text{matriciellement : } \begin{pmatrix}67\\ 4\end{pmatrix} = \begin{pmatrix}16 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}4\\ 3\end{pmatrix}\right) \\ 4 = 3 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}4\\ 3\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 1\end{pmatrix}\right) \\ 3 = 1 \times 3 + 0 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 1\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 67 et 4 est 1, c'est-à-dire : 4 est inversible modulo 67. Déduisons-en aussi des entiers u et v tels que : $67u + 4v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -16\end{pmatrix}\begin{pmatrix}67\\ 4\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & 17\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & 17\end{pmatrix}\begin{pmatrix}67\\ 4\end{pmatrix}$, c'est-à-dire : $67u + 4v = 1$, avec : $(u, v) = (-1{,}17)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 67, et on a : $4v \equiv 1 \bmod 67$. Ceci prouve que 4 admet pour inverse modulo 67 : $v = 17$. D'où le résultat.

Corrigé 8. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 1

$$\begin{cases} 161 = -10 \times (-16) + 1 \\ -10 = 1 \times (-10) + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 161 et -10 est 1, c'est-à-dire : -10 est inversible modulo 161. De plus la première division euclidienne implique immédiatement : $161u - 10v = 1$, avec : $(u, v) = (1{,}16)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 161, et on a : $-10v \equiv 1 \bmod 161$. Ceci prouve que -10 admet pour inverse modulo 161 : $v = 16$. D'où le résultat.

Corrigé 9. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour ← page 1

s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 27 = -4\times(-6)+3 & \left(\text{matriciellement : } \begin{pmatrix} 27 \\ -4 \end{pmatrix} = \begin{pmatrix} -6 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -4 \\ 3 \end{pmatrix}\right) \\ -4 = 3\times(-2)+2 & \left(\text{matriciellement : } \begin{pmatrix} -4 \\ 3 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}\right) \\ 3 = 2\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 27 et -4 est 1, c'est-à-dire : -4 est inversible modulo 27. Déduisons-en aussi des entiers u et v tels que : $27u+-4v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 6 \end{pmatrix}\begin{pmatrix} 27 \\ -4 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & -7 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -1 & -7 \end{pmatrix}\begin{pmatrix} 27 \\ -4 \end{pmatrix}$, c'est-à-dire : $27u-4v=1$, avec : $(u,v)=(-1,-7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 27, et on a : $-4v \equiv 1 \bmod 27$. Ceci prouve que -4 admet pour inverse modulo 27 : $v=-7$. D'où le résultat.

Corrigé 10. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases} 36 = 5\times 7+1 \\ 5 = 1\times 5+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 36 et 5 est 1, c'est-à-dire : 5 est inversible modulo 36. De plus la première division euclidienne implique immédiatement : $36u+5v=1$, avec : $(u,v)=(1,-7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 36, et on a : $5v \equiv 1 \bmod 36$. Ceci prouve que 5 admet pour inverse modulo 36 : $v=-7$. D'où le résultat.

Corrigé 11. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 1

$$\begin{cases} 906 = 43\times 21+3 & \left(\text{matriciellement : } \begin{pmatrix} 906 \\ 43 \end{pmatrix} = \begin{pmatrix} 21 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 43 \\ 3 \end{pmatrix}\right) \\ 43 = 3\times 14+1 & \left(\text{matriciellement : } \begin{pmatrix} 43 \\ 3 \end{pmatrix} = \begin{pmatrix} 14 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 1 \end{pmatrix}\right) \\ 3 = 1\times 3+0 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 906 et 43 est 1, c'est-à-dire : 43 est inversible modulo 906. Déduisons-en aussi des entiers u et v tels que : $906u+43v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -14\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -21\end{pmatrix}\begin{pmatrix}906\\ 43\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -14\end{pmatrix} \to \begin{pmatrix}-14 & 295\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -14 & 295 \end{pmatrix}\begin{pmatrix}906\\ 43\end{pmatrix}$, c'est-à-dire : $906u + 43v = 1$, avec : $(u, v) = (-14{,}295)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 906, et on a : $43v \equiv 1 \bmod 906$. Ceci prouve que 43 admet pour inverse modulo 906 : $v = 295$. D'où le résultat.

Corrigé 12. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases}
41 = -15 \times (-2) + 11 & \left(\text{matriciellement : } \begin{pmatrix}41\\ -15\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-15\\ 11\end{pmatrix}\right)\\
-15 = 11 \times (-2) + 7 & \left(\text{matriciellement : } \begin{pmatrix}-15\\ 11\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}11\\ 7\end{pmatrix}\right)\\
11 = 7 \times 1 + 4 & \left(\text{matriciellement : } \begin{pmatrix}11\\ 7\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}7\\ 4\end{pmatrix}\right)\\
7 = 4 \times 1 + 3 & \left(\text{matriciellement : } \begin{pmatrix}7\\ 4\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}4\\ 3\end{pmatrix}\right)\\
4 = 3 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}4\\ 3\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 1\end{pmatrix}\right)\\
3 = 1 \times 3 + 0 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 1\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 41 et -15 est 1, c'est-à-dire : -15 est inversible modulo 41. Déduisons-en aussi des entiers u et v tels que : $41u + -15v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}41\\ -15\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & 2\end{pmatrix} \to \begin{pmatrix}2 & -3\end{pmatrix} \to \begin{pmatrix}-3 & -4\end{pmatrix} \to \begin{pmatrix}-4 & -11\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -4 & -11 \end{pmatrix}\begin{pmatrix}41\\ -15\end{pmatrix}$, c'est-à-dire : $41u - 15v = 1$, avec : $(u, v) = (-4, -11)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 41, et on a : $-15v \equiv 1 \bmod 41$. Ceci prouve que -15 admet pour inverse modulo 41 : $v = -11$. D'où le résultat.

Corrigé 13. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On ← page 1

trouve successivement :

$$\begin{cases} 1639 = -5\times(-327)+4 & \left(\text{matriciellement : } \begin{pmatrix}1639\\-5\end{pmatrix} = \begin{pmatrix}-327 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-5\\4\end{pmatrix}\right) \\ -5 = 4\times(-2)+3 & \left(\text{matriciellement : } \begin{pmatrix}-5\\4\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}4\\3\end{pmatrix}\right) \\ 4 = 3\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix}4\\3\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\1\end{pmatrix}\right) \\ 3 = 1\times 3+0 & \left(\text{matriciellement : } \begin{pmatrix}3\\1\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 1639 et -5 est 1, c'est-à-dire : -5 est inversible modulo 1639. Déduisons-en aussi des entiers u et v tels que : $1639u + -5v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 327\end{pmatrix}\begin{pmatrix}1639\\-5\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -328\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & -328\end{pmatrix}\begin{pmatrix}1639\\-5\end{pmatrix}$, c'est-à-dire : $1639u - 5v = 1$, avec : $(u, v) = (-1, -328)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 1639, et on a : $-5v \equiv 1 \bmod 1639$. Ceci prouve que -5 admet pour inverse modulo 1639 : $v = -328$. D'où le résultat.

Corrigé 14. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 1

$$\begin{cases} 59 = -12\times(-4)+11 & \left(\text{matriciellement : } \begin{pmatrix}59\\-12\end{pmatrix} = \begin{pmatrix}-4 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-12\\11\end{pmatrix}\right) \\ -12 = 11\times(-2)+10 & \left(\text{matriciellement : } \begin{pmatrix}-12\\11\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}11\\10\end{pmatrix}\right) \\ 11 = 10\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix}11\\10\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}10\\1\end{pmatrix}\right) \\ 10 = 1\times 10+0 & \left(\text{matriciellement : } \begin{pmatrix}10\\1\end{pmatrix} = \begin{pmatrix}10 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 59 et -12 est 1, c'est-à-dire : -12 est inversible modulo 59. Déduisons-en aussi des entiers u et v tels que : $59u + -12v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -10\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 4\end{pmatrix}\begin{pmatrix}59\\-12\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -5\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & -5\end{pmatrix}\begin{pmatrix}59\\-12\end{pmatrix}$, c'est-à-dire : $59u - 12v = 1$, avec : $(u, v) = (-1, -5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 59, et on a : $-12v \equiv 1 \bmod 59$. Ceci prouve que -12 admet pour inverse modulo 59 : $v = -5$. D'où le résultat.

Corrigé 15. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve ← page 1

alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement :

$$\begin{cases} 91 = -43\times(-2)+5 & \left(\text{matriciellement : } \begin{pmatrix} 91 \\ -43 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -43 \\ 5 \end{pmatrix}\right) \\ -43 = 5\times(-9)+2 & \left(\text{matriciellement : } \begin{pmatrix} -43 \\ 5 \end{pmatrix} = \begin{pmatrix} -9 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 \\ 2 \end{pmatrix}\right) \\ 5 = 2\times 2+1 & \left(\text{matriciellement : } \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 91 et -43 est 1, c'est-à-dire : -43 est inversible modulo 91. Déduisons-en aussi des entiers u et v tels que : $91u + -43v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 9 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 91 \\ -43 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -2 \end{pmatrix} \to \begin{pmatrix} -2 & -17 \end{pmatrix} \to \begin{pmatrix} -17 & -36 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -17 & -36 \end{pmatrix}\begin{pmatrix} 91 \\ -43 \end{pmatrix}$, c'est-à-dire : $91u - 43v = 1$, avec : $(u, v) = (-17, -36)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 91, et on a : $-43v \equiv 1 \bmod 91$. Ceci prouve que -43 admet pour inverse modulo 91 : $v = -36$. D'où le résultat.

Corrigé 16. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 1

$$\begin{cases} 40 = 23\times 1+17 & \left(\text{matriciellement : } \begin{pmatrix} 40 \\ 23 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 23 \\ 17 \end{pmatrix}\right) \\ 23 = 17\times 1+6 & \left(\text{matriciellement : } \begin{pmatrix} 23 \\ 17 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 17 \\ 6 \end{pmatrix}\right) \\ 17 = 6\times 2+5 & \left(\text{matriciellement : } \begin{pmatrix} 17 \\ 6 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 6 \\ 5 \end{pmatrix}\right) \\ 6 = 5\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 6 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix}\right) \\ 5 = 1\times 5+0 & \left(\text{matriciellement : } \begin{pmatrix} 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 40 et 23 est 1, c'est-à-dire : 23 est inversible modulo 40. Déduisons-en aussi des entiers u et v tels que : $40u + 23v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 40 \\ 23 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & 3 \end{pmatrix} \to \begin{pmatrix} 3 & -4 \end{pmatrix} \to \begin{pmatrix} -4 & 7 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -4 & 7 \end{pmatrix}\begin{pmatrix} 40 \\ 23 \end{pmatrix}$, c'est-à-dire : $40u + 23v = 1$, avec : $(u, v) = (-4,7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 40, et on a : $23v \equiv 1 \bmod 40$. Ceci prouve que 23 admet pour inverse modulo 40 : $v = 7$. D'où le résultat.

Corrigé 17. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases} 34 &= 3\times 11+1 \\ 3 &= 1\times 3+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 34 et 3 est 1, c'est-à-dire : 3 est inversible modulo 34. De plus la première division euclidienne implique immédiatement : $34u+3v=1$, avec : $(u,v)=(1,-11)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 34, et on a : $3v\equiv 1 \bmod 34$. Ceci prouve que 3 admet pour inverse modulo 34 : $v=-11$. D'où le résultat.

Corrigé 18. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases} 16 &= -3\times(-5)+1 \\ -3 &= 1\times(-3)+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 16 et -3 est 1, c'est-à-dire : -3 est inversible modulo 16. De plus la première division euclidienne implique immédiatement : $16u-3v=1$, avec : $(u,v)=(1,5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 16, et on a : $-3v\equiv 1 \bmod 16$. Ceci prouve que -3 admet pour inverse modulo 16 : $v=5$. D'où le résultat.

Corrigé 19. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases} 23 &= 6\times 3+5 & \left(\text{matriciellement : } \begin{pmatrix} 23 \\ 6 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 6 \\ 5 \end{pmatrix}\right) \\ 6 &= 5\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 6 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix}\right) \\ 5 &= 1\times 5+0 & \left(\text{matriciellement : } \begin{pmatrix} 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 23 et 6 est 1, c'est-à-dire : 6 est inversible modulo 23. Déduisons-en aussi des entiers u et v tels que : $23u+6v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}\begin{pmatrix} 23 \\ 6 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & 4 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -1 & 4 \end{pmatrix}\begin{pmatrix} 23 \\ 6 \end{pmatrix}$, c'est-à-dire : $23u+6v=1$, avec : $(u,v)=(-1,4)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 23, et on a : $6v\equiv 1 \bmod 23$. Ceci prouve que 6 admet pour inverse modulo 23 : $v=4$. D'où le résultat.

Corrigé 20. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu ← page 1

la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 26 = 3\times 8+2 & \left(\text{matriciellement : } \begin{pmatrix} 26 \\ 3 \end{pmatrix} = \begin{pmatrix} 8 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}\right) \\ 3 = 2\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 26 et 3 est 1, c'est-à-dire : 3 est inversible modulo 26. Déduisons-en aussi des entiers u et v tels que : $26u+3v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix}\begin{pmatrix} 26 \\ 3 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & 9 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -1 & 9 \end{pmatrix}\begin{pmatrix} 26 \\ 3 \end{pmatrix}$, c'est-à-dire : $26u+3v=1$, avec : $(u,v)=(-1,9)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 26, et on a : $3v \equiv 1 \bmod 26$. Ceci prouve que 3 admet pour inverse modulo 26 : $v=9$. D'où le résultat.

Corrigé 21. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases} 49 = 3\times 16+1 \\ 3 = 1\times 3+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 49 et 3 est 1, c'est-à-dire : 3 est inversible modulo 49. De plus la première division euclidienne implique immédiatement : $49u+3v=1$, avec : $(u,v)=(1,-16)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 49, et on a : $3v \equiv 1 \bmod 49$. Ceci prouve que 3 admet pour inverse modulo 49 : $v=-16$. D'où le résultat.

Corrigé 22. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 1

$$\begin{cases} 17 = 3\times 5+2 & \left(\text{matriciellement : } \begin{pmatrix} 17 \\ 3 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}\right) \\ 3 = 2\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 17 et 3 est 1, c'est-à-dire : 3 est inversible modulo 17. Déduisons-en aussi des entiers u et v tels que : $17u+3v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}17\\ 3\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & 6\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & 6\end{pmatrix}\begin{pmatrix}17\\ 3\end{pmatrix}$, c'est-à-dire : $17u+3v = 1$, avec : $(u, v) = (-1{,}6)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 17, et on a : $3v \equiv 1 \bmod 17$. Ceci prouve que 3 admet pour inverse modulo 17 : $v = 6$. D'où le résultat.

Corrigé 23. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 1

$$\begin{cases}
367 = -8 \times (-45) + 7 & \left(\text{matriciellement : } \begin{pmatrix}367\\ -8\end{pmatrix} = \begin{pmatrix}-45 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-8\\ 7\end{pmatrix}\right)\\
-8 = 7 \times (-2) + 6 & \left(\text{matriciellement : } \begin{pmatrix}-8\\ 7\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}7\\ 6\end{pmatrix}\right)\\
7 = 6 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}7\\ 6\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}6\\ 1\end{pmatrix}\right)\\
6 = 1 \times 6 + 0 & \left(\text{matriciellement : } \begin{pmatrix}6\\ 1\end{pmatrix} = \begin{pmatrix}6 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 367 et -8 est 1, c'est-à-dire : -8 est inversible modulo 367. Déduisons-en aussi des entiers u et v tels que : $367u + -8v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -6\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 45\end{pmatrix}\begin{pmatrix}367\\ -8\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -46\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & -46\end{pmatrix}\begin{pmatrix}367\\ -8\end{pmatrix}$, c'est-à-dire : $367u-8v = 1$, avec : $(u, v) = (-1, -46)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 367, et on a : $-8v \equiv 1 \bmod 367$. Ceci prouve que -8 admet pour inverse modulo 367 : $v = -46$. D'où le résultat.

Corrigé 24. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 2

$$\begin{cases}
104 = -3 \times (-34) + 2 & \left(\text{matriciellement : } \begin{pmatrix}104\\ -3\end{pmatrix} = \begin{pmatrix}-34 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-3\\ 2\end{pmatrix}\right)\\
-3 = 2 \times (-2) + 1 & \left(\text{matriciellement : } \begin{pmatrix}-3\\ 2\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}\right)\\
2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix}2\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 104 et -3 est 1, c'est-à-dire : -3 est inversible modulo 104. Déduisons-en aussi des entiers u et v tels que : $104u + -3v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 34\end{pmatrix}\begin{pmatrix}104\\ -3\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & 2\end{pmatrix} \to \begin{pmatrix}2 & 69\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}2 & 69\end{pmatrix}\begin{pmatrix}104\\ -3\end{pmatrix}$, c'est-à-dire : $104u - 3v = 1$, avec : $(u, v) = (2{,}69)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 104, et on a : $-3v \equiv 1 \bmod 104$. Ceci prouve que -3 admet pour inverse modulo 104 : $v = 69$. D'où le résultat.

Corrigé 25. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 22 &= -3 \times (-7) + 1 \\ -3 &= 1 \times (-3) + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 22 et -3 est 1, c'est-à-dire : -3 est inversible modulo 22. De plus la première division euclidienne implique immédiatement : $22u - 3v = 1$, avec : $(u, v) = (1{,}7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 22, et on a : $-3v \equiv 1 \bmod 22$. Ceci prouve que -3 admet pour inverse modulo 22 : $v = 7$. D'où le résultat.

Corrigé 26. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 21 &= 5 \times 4 + 1 \\ 5 &= 1 \times 5 + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 21 et 5 est 1, c'est-à-dire : 5 est inversible modulo 21. De plus la première division euclidienne implique immédiatement : $21u + 5v = 1$, avec : $(u, v) = (1, -4)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 21, et on a : $5v \equiv 1 \bmod 21$. Ceci prouve que 5 admet pour inverse modulo 21 : $v = -4$. D'où le résultat.

Corrigé 27. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 27 &= -11 \times (-2) + 5 & \left(\text{matriciellement : } \begin{pmatrix}27\\ -11\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-11\\ 5\end{pmatrix}\right) \\ -11 &= 5 \times (-3) + 4 & \left(\text{matriciellement : } \begin{pmatrix}-11\\ 5\end{pmatrix} = \begin{pmatrix}-3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}5\\ 4\end{pmatrix}\right) \\ 5 &= 4 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}5\\ 4\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}4\\ 1\end{pmatrix}\right) \\ 4 &= 1 \times 4 + 0 & \left(\text{matriciellement : } \begin{pmatrix}4\\ 1\end{pmatrix} = \begin{pmatrix}4 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 27 et -11 est 1, c'est-à-dire : -11 est inversible modulo 27. Déduisons-en aussi des entiers u et v tels que : $27u + -11v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -4\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}27\\ -11\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -2\end{pmatrix} \to \begin{pmatrix}-2 & -5\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-2 & -5\end{pmatrix}\begin{pmatrix}27\\ -11\end{pmatrix}$, c'est-à-dire : $27u - 11v = 1$, avec : $(u, v) = (-2, -5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 27, et on a : $-11v \equiv 1 \bmod 27$. Ceci prouve que -11 admet pour inverse modulo 27 : $v = -5$. D'où le résultat.

Corrigé 28. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 2

$$\begin{cases}
379 = -4 \times (-94) + 3 & \left(\text{matriciellement : } \begin{pmatrix}379\\ -4\end{pmatrix} = \begin{pmatrix}-94 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-4\\ 3\end{pmatrix}\right)\\
-4 = 3 \times (-2) + 2 & \left(\text{matriciellement : } \begin{pmatrix}-4\\ 3\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 2\end{pmatrix}\right)\\
3 = 2 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 2\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}\right)\\
2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix}2\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 379 et -4 est 1, c'est-à-dire : -4 est inversible modulo 379. Déduisons-en aussi des entiers u et v tels que : $379u + -4v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 94\end{pmatrix}\begin{pmatrix}379\\ -4\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -95\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & -95\end{pmatrix}\begin{pmatrix}379\\ -4\end{pmatrix}$, c'est-à-dire : $379u - 4v = 1$, avec : $(u, v) = (-1, -95)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 379, et on a : $-4v \equiv 1 \bmod 379$. Ceci prouve que -4 admet pour inverse modulo 379 : $v = -95$. D'où le résultat.

Corrigé 29. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases}
23 = -10 \times (-2) + 3 & \left(\text{matriciellement : } \begin{pmatrix}23\\ -10\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-10\\ 3\end{pmatrix}\right)\\
-10 = 3 \times (-4) + 2 & \left(\text{matriciellement : } \begin{pmatrix}-10\\ 3\end{pmatrix} = \begin{pmatrix}-4 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 2\end{pmatrix}\right)\\
3 = 2 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 2\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}\right)\\
2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix}2\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 23 et -10 est 1, c'est-à-dire : -10 est inversible modulo 23. Déduisons-en aussi des entiers u et v tels que : $23u + -10v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 4\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}23\\ -10\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -3\end{pmatrix} \to \begin{pmatrix}-3 & -7\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-3 & -7\end{pmatrix}\begin{pmatrix}23\\ -10\end{pmatrix}$, c'est-à-dire : $23u - 10v = 1$, avec : $(u, v) = (-3, -7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 23, et on a : $-10v \equiv 1 \bmod 23$. Ceci prouve que -10 admet pour inverse modulo 23 : $v = -7$. D'où le résultat.

Corrigé 30. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 2

$$\begin{cases}
207 = -4 \times (-51) + 3 & \left(\text{matriciellement : } \begin{pmatrix}207\\ -4\end{pmatrix} = \begin{pmatrix}-51 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-4\\ 3\end{pmatrix}\right)\\
-4 = 3 \times (-2) + 2 & \left(\text{matriciellement : } \begin{pmatrix}-4\\ 3\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 2\end{pmatrix}\right)\\
3 = 2 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 2\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}\right)\\
2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix}2\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 207 et -4 est 1, c'est-à-dire : -4 est inversible modulo 207. Déduisons-en aussi des entiers u et v tels que : $207u + -4v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 51\end{pmatrix}\begin{pmatrix}207\\ -4\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -52\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & -52\end{pmatrix}\begin{pmatrix}207\\ -4\end{pmatrix}$, c'est-à-dire : $207u - 4v = 1$, avec : $(u, v) = (-1, -52)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 207, et on a : $-4v \equiv 1 \bmod 207$. Ceci prouve que -4 admet pour inverse modulo 207 : $v = -52$. D'où le résultat.

Corrigé 31. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 2

$$\begin{cases}
45 = 32 \times 1 + 13 & \left(\text{matriciellement : } \begin{pmatrix}45\\ 32\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}32\\ 13\end{pmatrix}\right)\\
32 = 13 \times 2 + 6 & \left(\text{matriciellement : } \begin{pmatrix}32\\ 13\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}13\\ 6\end{pmatrix}\right)\\
13 = 6 \times 2 + 1 & \left(\text{matriciellement : } \begin{pmatrix}13\\ 6\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}6\\ 1\end{pmatrix}\right)\\
6 = 1 \times 6 + 0 & \left(\text{matriciellement : } \begin{pmatrix}6\\ 1\end{pmatrix} = \begin{pmatrix}6 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 45 et 32 est 1, c'est-à-dire : 32 est inversible modulo 45. Déduisons-en aussi des entiers u et v tels que : $45u + 32v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -6\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}45\\ 32\end{pmatrix}$$
$$\searrow\quad\downarrow\qquad\downarrow\qquad\downarrow\qquad\downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix}\to\begin{pmatrix}1 & -2\end{pmatrix}\to\begin{pmatrix}-2 & 5\end{pmatrix}\to\begin{pmatrix}5 & -7\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}5 & -7\end{pmatrix}\begin{pmatrix}45\\ 32\end{pmatrix}$, c'est-à-dire : $45u + 32v = 1$, avec : $(u, v) = (5, -7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 45, et on a : $32v \equiv 1 \bmod 45$. Ceci prouve que 32 admet pour inverse modulo 45 : $v = -7$. D'où le résultat.

Corrigé 32. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 41 = 7\times 5 + 6 & \left(\text{matriciellement : } \begin{pmatrix}41\\ 7\end{pmatrix} = \begin{pmatrix}5 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}7\\ 6\end{pmatrix}\right)\\ 7 = 6\times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}7\\ 6\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}6\\ 1\end{pmatrix}\right)\\ 6 = 1\times 6 + 0 & \left(\text{matriciellement : } \begin{pmatrix}6\\ 1\end{pmatrix} = \begin{pmatrix}6 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 41 et 7 est 1, c'est-à-dire : 7 est inversible modulo 41. Déduisons-en aussi des entiers u et v tels que : $41u + 7v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -6\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}41\\ 7\end{pmatrix}$$
$$\searrow\quad\downarrow\qquad\downarrow\qquad\downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix}\to\begin{pmatrix}1 & -1\end{pmatrix}\to\begin{pmatrix}-1 & 6\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & 6\end{pmatrix}\begin{pmatrix}41\\ 7\end{pmatrix}$, c'est-à-dire : $41u+7v = 1$, avec : $(u, v) = (-1,6)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 41, et on a : $7v \equiv 1 \bmod 41$. Ceci prouve que 7 admet pour inverse modulo 41 : $v = 6$. D'où le résultat.

Corrigé 33. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 25 = 3\times 8 + 1\\ 3 = 1\times 3 + 0\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 25 et 3 est 1, c'est-à-dire : 3 est inversible modulo 25. De plus la première division euclidienne implique immédiatement : $25u + 3v = 1$, avec : $(u, v) = (1, -8)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 25, et on a : $3v \equiv 1 \bmod 25$. Ceci prouve que 3 admet pour inverse modulo 25 : $v = -8$. D'où le résultat.

Corrigé 34. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 2

$$\begin{cases} 58 = 3\times 19 + 1\\ 3 = 1\times 3 + 0\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 58 et 3 est 1, c'est-à-dire : 3 est inversible modulo 58. De plus la première division euclidienne implique immédiatement : $58u + 3v = 1$, avec : $(u, v) = (1, -19)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 58, et on a : $3v \equiv 1 \bmod 58$. Ceci prouve que 3 admet pour inverse modulo 58 : $v = -19$. D'où le résultat.

Corrigé 35. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 47 = 6 \times 7 + 5 & \left(\text{matriciellement : } \begin{pmatrix} 47 \\ 6 \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 6 \\ 5 \end{pmatrix} \right) \\ 6 = 5 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix} 6 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 5 \\ 1 \end{pmatrix} \right) \\ 5 = 1 \times 5 + 0 & \left(\text{matriciellement : } \begin{pmatrix} 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 47 et 6 est 1, c'est-à-dire : 6 est inversible modulo 47. Déduisons-en aussi des entiers u et v tels que : $47u + 6v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -7 \end{pmatrix} \begin{pmatrix} 47 \\ 6 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & 8 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -1 & 8 \end{pmatrix} \begin{pmatrix} 47 \\ 6 \end{pmatrix}$, c'est-à-dire : $47u + 6v = 1$, avec : $(u, v) = (-1,8)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 47, et on a : $6v \equiv 1 \bmod 47$. Ceci prouve que 6 admet pour inverse modulo 47 : $v = 8$. D'où le résultat.

Corrigé 36. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 2

$$\begin{cases} 79 = -3 \times (-26) + 1 \\ -3 = 1 \times (-3) + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 79 et -3 est 1, c'est-à-dire : -3 est inversible modulo 79. De plus la première division euclidienne implique immédiatement : $79u - 3v = 1$, avec : $(u, v) = (1,26)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 79, et on a : $-3v \equiv 1 \bmod 79$. Ceci prouve que -3 admet pour inverse modulo 79 : $v = 26$. D'où le résultat.

Corrigé 37. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 17 = 5 \times 3 + 2 & \left(\text{matriciellement : } \begin{pmatrix} 17 \\ 5 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 5 \\ 2 \end{pmatrix} \right) \\ 5 = 2 \times 2 + 1 & \left(\text{matriciellement : } \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right) \\ 2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 17 et 5 est 1, c'est-à-dire : 5 est inversible modulo 17. Déduisons-en aussi des entiers u et v tels que : $17u + 5v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}17\\ 5\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -2\end{pmatrix} \to \begin{pmatrix}-2 & 7\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-2 & 7\end{pmatrix}\begin{pmatrix}17\\ 5\end{pmatrix}$, c'est-à-dire : $17u+5v = 1$, avec : $(u, v) = (-2{,}7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 17, et on a : $5v \equiv 1 \bmod 17$. Ceci prouve que 5 admet pour inverse modulo 17 : $v = 7$. D'où le résultat.

Corrigé 38. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 2

$$\begin{cases} 92 &= 7 \times 13 + 1 \\ 7 &= 1 \times 7 + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 92 et 7 est 1, c'est-à-dire : 7 est inversible modulo 92. De plus la première division euclidienne implique immédiatement : $92u + 7v = 1$, avec : $(u, v) = (1, -13)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 92, et on a : $7v \equiv 1 \bmod 92$. Ceci prouve que 7 admet pour inverse modulo 92 : $v = -13$. D'où le résultat.

Corrigé 39. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 22 = -5 \times (-4) + 2 & \left(\text{matriciellement : } \begin{pmatrix}22\\ -5\end{pmatrix} = \begin{pmatrix}-4 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-5\\ 2\end{pmatrix}\right) \\ -5 = 2 \times (-3) + 1 & \left(\text{matriciellement : } \begin{pmatrix}-5\\ 2\end{pmatrix} = \begin{pmatrix}-3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}\right) \\ 2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix}2\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 22 et -5 est 1, c'est-à-dire : -5 est inversible modulo 22. Déduisons-en aussi des entiers u et v tels que : $22u + -5v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 4\end{pmatrix}\begin{pmatrix}22\\ -5\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & 3\end{pmatrix} \to \begin{pmatrix}3 & 13\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}3 & 13\end{pmatrix}\begin{pmatrix}22\\ -5\end{pmatrix}$, c'est-à-dire : $22u - 5v = 1$, avec : $(u, v) = (3{,}13)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 22, et on a : $-5v \equiv 1 \bmod 22$. Ceci prouve que -5 admet pour inverse modulo 22 : $v = 13$. D'où le résultat.

Corrigé 40. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour ← page 2

s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 23 = -10\times(-2)+3 & \left(\text{matriciellement : } \begin{pmatrix} 23 \\ -10 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -10 \\ 3 \end{pmatrix}\right) \\ -10 = 3\times(-4)+2 & \left(\text{matriciellement : } \begin{pmatrix} -10 \\ 3 \end{pmatrix} = \begin{pmatrix} -4 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}\right) \\ 3 = 2\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 23 et -10 est 1, c'est-à-dire : -10 est inversible modulo 23. Déduisons-en aussi des entiers u et v tels que : $23u + -10v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 23 \\ -10 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & -3 \end{pmatrix} \to \begin{pmatrix} -3 & -7 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -3 & -7 \end{pmatrix}\begin{pmatrix} 23 \\ -10 \end{pmatrix}$, c'est-à-dire : $23u - 10v = 1$, avec : $(u, v) = (-3, -7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 23, et on a : $-10v \equiv 1 \bmod 23$. Ceci prouve que -10 admet pour inverse modulo 23 : $v = -7$. D'où le résultat.

Corrigé 41. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 21 = -13\times(-1)+8 & \left(\text{matriciellement : } \begin{pmatrix} 21 \\ -13 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -13 \\ 8 \end{pmatrix}\right) \\ -13 = 8\times(-2)+3 & \left(\text{matriciellement : } \begin{pmatrix} -13 \\ 8 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 8 \\ 3 \end{pmatrix}\right) \\ 8 = 3\times 2+2 & \left(\text{matriciellement : } \begin{pmatrix} 8 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}\right) \\ 3 = 2\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 21 et -13 est 1, c'est-à-dire : -13 est inversible modulo 21. Déduisons-en aussi des entiers u et v tels que : $21u + -13v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 21 \\ -13 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & 3 \end{pmatrix} \to \begin{pmatrix} 3 & 5 \end{pmatrix} \to \begin{pmatrix} 5 & 8 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} 5 & 8 \end{pmatrix}\begin{pmatrix} 21 \\ -13 \end{pmatrix}$, c'est-à-dire : $21u - 13v = 1$, avec : $(u, v) = (5,8)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 21, et on a : $-13v \equiv 1 \bmod 21$. Ceci prouve que -13 admet pour inverse modulo 21 : $v = 8$. D'où le résultat.

Corrigé 42. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 2

$$\begin{cases} 51 = -20\times(-2)+11 & \left(\text{matriciellement : } \begin{pmatrix} 51 \\ -20 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -20 \\ 11 \end{pmatrix}\right) \\ -20 = 11\times(-2)+2 & \left(\text{matriciellement : } \begin{pmatrix} -20 \\ 11 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 11 \\ 2 \end{pmatrix}\right) \\ 11 = 2\times 5+1 & \left(\text{matriciellement : } \begin{pmatrix} 11 \\ 2 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 51 et -20 est 1, c'est-à-dire : -20 est inversible modulo 51. Déduisons-en aussi des entiers u et v tels que : $51u + -20v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 51 \\ -20 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -5 \end{pmatrix} \to \begin{pmatrix} -5 & -9 \end{pmatrix} \to \begin{pmatrix} -9 & -23 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -9 & -23 \end{pmatrix}\begin{pmatrix} 51 \\ -20 \end{pmatrix}$, c'est-à-dire : $51u - 20v = 1$, avec : $(u, v) = (-9, -23)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 51, et on a : $-20v \equiv 1 \bmod 51$. Ceci prouve que -20 admet pour inverse modulo 51 : $v = -23$. D'où le résultat.

Corrigé 43. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 2

$$\begin{cases} 53 = -7\times(-7)+4 & \left(\text{matriciellement : } \begin{pmatrix} 53 \\ -7 \end{pmatrix} = \begin{pmatrix} -7 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -7 \\ 4 \end{pmatrix}\right) \\ -7 = 4\times(-2)+1 & \left(\text{matriciellement : } \begin{pmatrix} -7 \\ 4 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 4 \\ 1 \end{pmatrix}\right) \\ 4 = 1\times 4+0 & \left(\text{matriciellement : } \begin{pmatrix} 4 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 53 et -7 est 1, c'est-à-dire : -7 est inversible modulo 53. Déduisons-en aussi des entiers u et v tels que : $53u + -7v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 7 \end{pmatrix}\begin{pmatrix} 53 \\ -7 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 15 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} 2 & 15 \end{pmatrix}\begin{pmatrix} 53 \\ -7 \end{pmatrix}$, c'est-à-dire : $53u - 7v = 1$, avec : $(u, v) = (2,15)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 53, et on a : $-7v \equiv 1 \bmod 53$. Ceci prouve que -7 admet pour inverse modulo 53 : $v = 15$. D'où le résultat.

Corrigé 44. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu ← page 2

la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 19 &= -3 \times (-6) + 1 \\ -3 &= 1 \times (-3) + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 19 et -3 est 1, c'est-à-dire : -3 est inversible modulo 19. De plus la première division euclidienne implique immédiatement : $19u - 3v = 1$, avec : $(u, v) = (1{,}6)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 19, et on a : $-3v \equiv 1 \bmod 19$. Ceci prouve que -3 admet pour inverse modulo 19 : $v = 6$. D'où le résultat.

Corrigé 45. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 33 &= -20 \times (-1) + 13 & \left(\text{matriciellement : } \begin{pmatrix} 33 \\ -20 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -20 \\ 13 \end{pmatrix}\right) \\ -20 &= 13 \times (-2) + 6 & \left(\text{matriciellement : } \begin{pmatrix} -20 \\ 13 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 13 \\ 6 \end{pmatrix}\right) \\ 13 &= 6 \times 2 + 1 & \left(\text{matriciellement : } \begin{pmatrix} 13 \\ 6 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 6 \\ 1 \end{pmatrix}\right) \\ 6 &= 1 \times 6 + 0 & \left(\text{matriciellement : } \begin{pmatrix} 6 \\ 1 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 33 et -20 est 1, c'est-à-dire : -20 est inversible modulo 33. Déduisons-en aussi des entiers u et v tels que : $33u + -20v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 33 \\ -20 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -2 \end{pmatrix} \to \begin{pmatrix} -2 & -3 \end{pmatrix} \to \begin{pmatrix} -3 & -5 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -3 & -5 \end{pmatrix} \begin{pmatrix} 33 \\ -20 \end{pmatrix}$, c'est-à-dire : $33u - 20v = 1$, avec : $(u, v) = (-3, -5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 33, et on a : $-20v \equiv 1 \bmod 33$. Ceci prouve que -20 admet pour inverse modulo 33 : $v = -5$. D'où le résultat.

Corrigé 46. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 31 &= -3 \times (-10) + 1 \\ -3 &= 1 \times (-3) + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 31 et -3 est 1, c'est-à-dire : -3 est inversible modulo 31. De plus la première division euclidienne implique immédiatement : $31u - 3v = 1$, avec : $(u, v) = (1{,}10)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 31, et on a : $-3v \equiv 1 \bmod 31$. Ceci prouve que -3 admet pour inverse modulo 31 : $v = 10$. D'où le résultat.

Corrigé 47. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu ← page 2

la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 37 &= -17\times(-2)+3 & \left(\text{matriciellement : } \begin{pmatrix} 37 \\ -17 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -17 \\ 3 \end{pmatrix}\right) \\ -17 &= 3\times(-6)+1 & \left(\text{matriciellement : } \begin{pmatrix} -17 \\ 3 \end{pmatrix} = \begin{pmatrix} -6 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 1 \end{pmatrix}\right) \\ 3 &= 1\times 3+0 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 37 et -17 est 1, c'est-à-dire : -17 est inversible modulo 37. Déduisons-en aussi des entiers u et v tels que : $37u + -17v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 6 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 37 \\ -17 \end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 6 \end{pmatrix} \to \begin{pmatrix} 6 & 13 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} 6 & 13 \end{pmatrix}\begin{pmatrix} 37 \\ -17 \end{pmatrix}$, c'est-à-dire : $37u - 17v = 1$, avec : $(u, v) = (6{,}13)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 37, et on a : $-17v \equiv 1 \bmod 37$. Ceci prouve que -17 admet pour inverse modulo 37 : $v = 13$. D'où le résultat.

Corrigé 48. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 2

$$\begin{cases} 113 &= -3\times(-37)+2 & \left(\text{matriciellement : } \begin{pmatrix} 113 \\ -3 \end{pmatrix} = \begin{pmatrix} -37 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -3 \\ 2 \end{pmatrix}\right) \\ -3 &= 2\times(-2)+1 & \left(\text{matriciellement : } \begin{pmatrix} -3 \\ 2 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 &= 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 113 et -3 est 1, c'est-à-dire : -3 est inversible modulo 113. Déduisons-en aussi des entiers u et v tels que : $113u + -3v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 37 \end{pmatrix}\begin{pmatrix} 113 \\ -3 \end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 75 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} 2 & 75 \end{pmatrix}\begin{pmatrix} 113 \\ -3 \end{pmatrix}$, c'est-à-dire : $113u - 3v = 1$, avec : $(u, v) = (2{,}75)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 113, et on a : $-3v \equiv 1 \bmod 113$. Ceci prouve que -3 admet pour inverse modulo 113 : $v = 75$. D'où le résultat.

Corrigé 49. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 25 &= 4\times 6+1 \\ 4 &= 1\times 4+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 25 et 4 est 1, c'est-à-dire : 4 est inversible modulo 25. De plus la première division euclidienne implique immédiatement : $25u + 4v = 1$, avec : $(u, v) = (1, -6)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 25, et on a : $4v \equiv 1 \bmod 25$. Ceci prouve que 4 admet pour inverse modulo 25 : $v = -6$. D'où le résultat.

Corrigé 50. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 2

$$\begin{cases} 17 = 5 \times 3 + 2 & \left(\text{matriciellement : } \begin{pmatrix} 17 \\ 5 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 5 \\ 2 \end{pmatrix} \right) \\ 5 = 2 \times 2 + 1 & \left(\text{matriciellement : } \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right) \\ 2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 17 et 5 est 1, c'est-à-dire : 5 est inversible modulo 17. Déduisons-en aussi des entiers u et v tels que : $17u + 5v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 17 \\ 5 \end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -2 \end{pmatrix} \to \begin{pmatrix} -2 & 7 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -2 & 7 \end{pmatrix} \begin{pmatrix} 17 \\ 5 \end{pmatrix}$, c'est-à-dire : $17u + 5v = 1$, avec : $(u, v) = (-2,7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 17, et on a : $5v \equiv 1 \bmod 17$. Ceci prouve que 5 admet pour inverse modulo 17 : $v = 7$. D'où le résultat.

Corrigé 51. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases} 172 = 7 \times 24 + 4 & \left(\text{matriciellement : } \begin{pmatrix} 172 \\ 7 \end{pmatrix} = \begin{pmatrix} 24 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} \right) \\ 7 = 4 \times 1 + 3 & \left(\text{matriciellement : } \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 \\ 3 \end{pmatrix} \right) \\ 4 = 3 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} \right) \\ 3 = 1 \times 3 + 0 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 172 et 7 est 1, c'est-à-dire : 7 est inversible modulo 172. Déduisons-en aussi des entiers u et v tels que : $172u + 7v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -24 \end{pmatrix} \begin{pmatrix} 172 \\ 7 \end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & -49 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} 2 & -49 \end{pmatrix} \begin{pmatrix} 172 \\ 7 \end{pmatrix}$, c'est-à-dire : $172u + 7v = 1$, avec : $(u, v) = (2, -49)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 172, et on a : $7v \equiv 1 \bmod 172$. Ceci prouve que 7 admet pour inverse modulo 172 : $v = -49$. D'où le résultat.

Corrigé 52. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases} 169 = -19 \times (-8) + 17 & \left(\text{matriciellement : } \begin{pmatrix} 169 \\ -19 \end{pmatrix} = \begin{pmatrix} -8 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -19 \\ 17 \end{pmatrix} \right) \\ -19 = 17 \times (-2) + 15 & \left(\text{matriciellement : } \begin{pmatrix} -19 \\ 17 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 17 \\ 15 \end{pmatrix} \right) \\ 17 = 15 \times 1 + 2 & \left(\text{matriciellement : } \begin{pmatrix} 17 \\ 15 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 15 \\ 2 \end{pmatrix} \right) \\ 15 = 2 \times 7 + 1 & \left(\text{matriciellement : } \begin{pmatrix} 15 \\ 2 \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right) \\ 2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 169 et -19 est 1, c'est-à-dire : -19 est inversible modulo 169. Déduisons-en aussi des entiers u et v tels que : $169u + -19v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -7 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 8 \end{pmatrix} \begin{pmatrix} 169 \\ -19 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -7 \end{pmatrix} \to \begin{pmatrix} -7 & 8 \end{pmatrix} \to \begin{pmatrix} 8 & 9 \end{pmatrix} \to \begin{pmatrix} 9 & 80 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} 9 & 80 \end{pmatrix} \begin{pmatrix} 169 \\ -19 \end{pmatrix}$, c'est-à-dire : $169u - 19v = 1$, avec : $(u, v) = (9{,}80)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 169, et on a : $-19v \equiv 1 \bmod 169$. Ceci prouve que -19 admet pour inverse modulo 169 : $v = 80$. D'où le résultat.

Corrigé 53. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 3

$$\begin{cases} 16 = -3 \times (-5) + 1 \\ -3 = 1 \times (-3) + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 16 et -3 est 1, c'est-à-dire : -3 est inversible modulo 16. De plus la première division euclidienne implique immédiatement : $16u - 3v = 1$, avec : $(u, v) = (1{,}5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 16, et on a : $-3v \equiv 1 \bmod 16$. Ceci prouve que -3 admet pour inverse modulo 16 : $v = 5$. D'où le résultat.

Corrigé 54. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour ← page 3

s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 27 = 10\times 2+7 & \left(\text{matriciellement : } \begin{pmatrix}27\\10\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}10\\7\end{pmatrix}\right)\\ 10 = 7\times 1+3 & \left(\text{matriciellement : } \begin{pmatrix}10\\7\end{pmatrix}=\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}7\\3\end{pmatrix}\right)\\ 7 = 3\times 2+1 & \left(\text{matriciellement : } \begin{pmatrix}7\\3\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}3\\1\end{pmatrix}\right)\\ 3 = 1\times 3+0 & \left(\text{matriciellement : } \begin{pmatrix}3\\1\end{pmatrix}=\begin{pmatrix}3&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 27 et 10 est 1, c'est-à-dire : 10 est inversible modulo 27. Déduisons-en aussi des entiers u et v tels que : $27u+10v=1$. Les relations matricielles ci-dessus impliquent :

$$1=\begin{pmatrix}1&0\end{pmatrix}\begin{pmatrix}0&1\\1&-3\end{pmatrix}\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}27\\10\end{pmatrix}$$
$$\begin{pmatrix}0&1\end{pmatrix}\to\begin{pmatrix}1&-2\end{pmatrix}\to\begin{pmatrix}-2&3\end{pmatrix}\to\begin{pmatrix}3&-8\end{pmatrix}$$

En résumé on a : $1=\begin{pmatrix}3&-8\end{pmatrix}\begin{pmatrix}27\\10\end{pmatrix}$, c'est-à-dire : $27u+10v=1$, avec : $(u,v)=(3,-8)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 27, et on a : $10v\equiv 1 \bmod 27$. Ceci prouve que 10 admet pour inverse modulo 27 : $v=-8$. D'où le résultat.

Corrigé 55. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). ← page 3 On trouve successivement :

$$\begin{cases} 25 = 3\times 8+1\\ 3 = 1\times 3+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 25 et 3 est 1, c'est-à-dire : 3 est inversible modulo 25. De plus la première division euclidienne implique immédiatement : $25u+3v=1$, avec : $(u,v)=(1,-8)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 25, et on a : $3v\equiv 1 \bmod 25$. Ceci prouve que 3 admet pour inverse modulo 25 : $v=-8$. D'où le résultat.

Corrigé 56. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). ← page 3 On trouve successivement :

$$\begin{cases} 47 = 9\times 5+2 & \left(\text{matriciellement : } \begin{pmatrix}47\\9\end{pmatrix}=\begin{pmatrix}5&1\\1&0\end{pmatrix}\begin{pmatrix}9\\2\end{pmatrix}\right)\\ 9 = 2\times 4+1 & \left(\text{matriciellement : } \begin{pmatrix}9\\2\end{pmatrix}=\begin{pmatrix}4&1\\1&0\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix}\right)\\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix}2\\1\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 47 et 9 est 1, c'est-à-dire : 9 est inversible modulo 47. Déduisons-en aussi des entiers u et v tels que : $47u+9v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -4\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}47\\ 9\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -4\end{pmatrix} \to \begin{pmatrix}-4 & 21\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-4 & 21\end{pmatrix}\begin{pmatrix}47\\ 9\end{pmatrix}$, c'est-à-dire : $47u + 9v = 1$, avec : $(u, v) = (-4{,}21)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 47, et on a : $9v \equiv 1 \bmod 47$. Ceci prouve que 9 admet pour inverse modulo 47 : $v = 21$. D'où le résultat.

Corrigé 57. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 3

$$\begin{cases}
18 = -5 \times (-3) + 3 & \left(\text{matriciellement : } \begin{pmatrix}18\\ -5\end{pmatrix} = \begin{pmatrix}-3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-5\\ 3\end{pmatrix}\right)\\
-5 = 3 \times (-2) + 1 & \left(\text{matriciellement : } \begin{pmatrix}-5\\ 3\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 1\end{pmatrix}\right)\\
3 = 1 \times 3 + 0 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 1\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 18 et -5 est 1, c'est-à-dire : -5 est inversible modulo 18. Déduisons-en aussi des entiers u et v tels que : $18u + -5v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 3\end{pmatrix}\begin{pmatrix}18\\ -5\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & 2\end{pmatrix} \to \begin{pmatrix}2 & 7\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}2 & 7\end{pmatrix}\begin{pmatrix}18\\ -5\end{pmatrix}$, c'est-à-dire : $18u - 5v = 1$, avec : $(u, v) = (2{,}7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 18, et on a : $-5v \equiv 1 \bmod 18$. Ceci prouve que -5 admet pour inverse modulo 18 : $v = 7$. D'où le résultat.

Corrigé 58. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases}
275 = 67 \times 4 + 7 & \left(\text{matriciellement : } \begin{pmatrix}275\\ 67\end{pmatrix} = \begin{pmatrix}4 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}67\\ 7\end{pmatrix}\right)\\
67 = 7 \times 9 + 4 & \left(\text{matriciellement : } \begin{pmatrix}67\\ 7\end{pmatrix} = \begin{pmatrix}9 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}7\\ 4\end{pmatrix}\right)\\
7 = 4 \times 1 + 3 & \left(\text{matriciellement : } \begin{pmatrix}7\\ 4\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}4\\ 3\end{pmatrix}\right)\\
4 = 3 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}4\\ 3\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 1\end{pmatrix}\right)\\
3 = 1 \times 3 + 0 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 1\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 275 et 67 est 1, c'est-à-dire : 67 est inversible modulo 275. Déduisons-en aussi des entiers u et v tels que : $275u + 67v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -9\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -4\end{pmatrix}\begin{pmatrix}275\\ 67\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & 2\end{pmatrix} \to \begin{pmatrix}2 & -19\end{pmatrix} \to \begin{pmatrix}-19 & 78\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-19 & 78\end{pmatrix}\begin{pmatrix}275\\ 67\end{pmatrix}$, c'est-à-dire : $275u + 67v = 1$, avec : $(u, v) = (-19{,}78)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 275, et on a : $67v \equiv 1 \bmod 275$. Ceci prouve que 67 admet pour inverse modulo 275 : $v = 78$. D'où le résultat.

Corrigé 59. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases}
131 = -11 \times (-11) + 10 & \left(\text{matriciellement : } \begin{pmatrix}131\\ -11\end{pmatrix} = \begin{pmatrix}-11 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-11\\ 10\end{pmatrix}\right)\\
-11 = 10 \times (-2) + 9 & \left(\text{matriciellement : } \begin{pmatrix}-11\\ 10\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}10\\ 9\end{pmatrix}\right)\\
10 = 9 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}10\\ 9\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}9\\ 1\end{pmatrix}\right)\\
9 = 1 \times 9 + 0 & \left(\text{matriciellement : } \begin{pmatrix}9\\ 1\end{pmatrix} = \begin{pmatrix}9 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 131 et -11 est 1, c'est-à-dire : -11 est inversible modulo 131. Déduisons-en aussi des entiers u et v tels que : $131u + -11v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -9\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 11\end{pmatrix}\begin{pmatrix}131\\ -11\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -12\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & -12\end{pmatrix}\begin{pmatrix}131\\ -11\end{pmatrix}$, c'est-à-dire : $131u - 11v = 1$, avec : $(u, v) = (-1, -12)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 131, et on a : $-11v \equiv 1 \bmod 131$. Ceci prouve que -11 admet pour inverse modulo 131 : $v = -12$. D'où le résultat.

Corrigé 60. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases}
175 = -4 \times (-43) + 3 & \left(\text{matriciellement : } \begin{pmatrix}175\\ -4\end{pmatrix} = \begin{pmatrix}-43 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-4\\ 3\end{pmatrix}\right)\\
-4 = 3 \times (-2) + 2 & \left(\text{matriciellement : } \begin{pmatrix}-4\\ 3\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 2\end{pmatrix}\right)\\
3 = 2 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 2\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}\right)\\
2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix}2\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 175 et -4 est 1, c'est-à-dire : -4 est inversible modulo 175. Déduisons-en aussi des entiers u et v tels que : $175u + -4v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 43\end{pmatrix}\begin{pmatrix}175\\ -4\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -44\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & -44\end{pmatrix}\begin{pmatrix}175\\ -4\end{pmatrix}$, c'est-à-dire : $175u - 4v = 1$, avec : $(u, v) = (-1, -44)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 175, et on a : $-4v \equiv 1 \bmod 175$. Ceci prouve que -4 admet pour inverse modulo 175 : $v = -44$. D'où le résultat.

Corrigé 61. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases}
59 = -7 \times (-8) + 3 & \left(\text{matriciellement : } \begin{pmatrix}59\\ -7\end{pmatrix} = \begin{pmatrix}-8 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-7\\ 3\end{pmatrix}\right)\\
-7 = 3 \times (-3) + 2 & \left(\text{matriciellement : } \begin{pmatrix}-7\\ 3\end{pmatrix} = \begin{pmatrix}-3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 2\end{pmatrix}\right)\\
3 = 2 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 2\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}\right)\\
2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix}2\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 59 et -7 est 1, c'est-à-dire : -7 est inversible modulo 59. Déduisons-en aussi des entiers u et v tels que : $59u + -7v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 8\end{pmatrix}\begin{pmatrix}59\\ -7\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -2\end{pmatrix} \to \begin{pmatrix}-2 & -17\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-2 & -17\end{pmatrix}\begin{pmatrix}59\\ -7\end{pmatrix}$, c'est-à-dire : $59u - 7v = 1$, avec : $(u, v) = (-2, -17)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 59, et on a : $-7v \equiv 1 \bmod 59$. Ceci prouve que -7 admet pour inverse modulo 59 : $v = -17$. D'où le résultat.

Corrigé 62. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 3

$$\begin{cases}
29 = 4 \times 7 + 1\\
4 = 1 \times 4 + 0
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 29 et 4 est 1, c'est-à-dire : 4 est inversible modulo 29. De plus la première division euclidienne implique immédiatement : $29u + 4v = 1$, avec : $(u, v) = (1, -7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 29, et on a : $4v \equiv 1 \bmod 29$. Ceci prouve que 4 admet pour inverse modulo 29 : $v = -7$. D'où le résultat.

Corrigé 63. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour ← page 3

s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 31 &= -5\times(-6)+1 \\ -5 &= 1\times(-5)+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 31 et -5 est 1, c'est-à-dire : -5 est inversible modulo 31. De plus la première division euclidienne implique immédiatement : $31u-5v=1$, avec : $(u,v)=(1{,}6)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 31, et on a : $-5v\equiv 1 \bmod 31$. Ceci prouve que -5 admet pour inverse modulo 31 : $v=6$. D'où le résultat.

Corrigé 64. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases} 114 &= -17\times(-6)+12 & \left(\text{matriciellement : } \begin{pmatrix}114\\-17\end{pmatrix}=\begin{pmatrix}-6&1\\1&0\end{pmatrix}\begin{pmatrix}-17\\12\end{pmatrix}\right) \\ -17 &= 12\times(-2)+7 & \left(\text{matriciellement : } \begin{pmatrix}-17\\12\end{pmatrix}=\begin{pmatrix}-2&1\\1&0\end{pmatrix}\begin{pmatrix}12\\7\end{pmatrix}\right) \\ 12 &= 7\times 1+5 & \left(\text{matriciellement : } \begin{pmatrix}12\\7\end{pmatrix}=\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}7\\5\end{pmatrix}\right) \\ 7 &= 5\times 1+2 & \left(\text{matriciellement : } \begin{pmatrix}7\\5\end{pmatrix}=\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}5\\2\end{pmatrix}\right) \\ 5 &= 2\times 2+1 & \left(\text{matriciellement : } \begin{pmatrix}5\\2\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix}\right) \\ 2 &= 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix}2\\1\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 114 et -17 est 1, c'est-à-dire : -17 est inversible modulo 114. Déduisons-en aussi des entiers u et v tels que : $114u+-17v=1$. Les relations matricielles ci-dessus impliquent :

$$1=\begin{pmatrix}1&0\end{pmatrix}\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&2\end{pmatrix}\begin{pmatrix}0&1\\1&6\end{pmatrix}\begin{pmatrix}114\\-17\end{pmatrix}$$

$$\begin{pmatrix}0&1\end{pmatrix}\to\begin{pmatrix}1&-2\end{pmatrix}\to\begin{pmatrix}-2&3\end{pmatrix}\to\begin{pmatrix}3&-5\end{pmatrix}\to\begin{pmatrix}-5&-7\end{pmatrix}\to\begin{pmatrix}-7&-47\end{pmatrix}$$

En résumé on a : $1=\begin{pmatrix}-7&-47\end{pmatrix}\begin{pmatrix}114\\-17\end{pmatrix}$, c'est-à-dire : $114u-17v=1$, avec : $(u,v)=(-7,-47)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 114, et on a : $-17v\equiv 1 \bmod 114$. Ceci prouve que -17 admet pour inverse modulo 114 : $v=-47$. D'où le résultat.

Corrigé 65. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 3

$$\begin{cases} 20 &= -3\times(-6)+2 & \left(\text{matriciellement : } \begin{pmatrix}20\\-3\end{pmatrix}=\begin{pmatrix}-6&1\\1&0\end{pmatrix}\begin{pmatrix}-3\\2\end{pmatrix}\right) \\ -3 &= 2\times(-2)+1 & \left(\text{matriciellement : } \begin{pmatrix}-3\\2\end{pmatrix}=\begin{pmatrix}-2&1\\1&0\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix}\right) \\ 2 &= 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix}2\\1\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 20 et -3 est 1, c'est-à-dire : -3 est inversible modulo 20. Déduisons-en aussi des entiers u et v tels que : $20u + -3v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 6\end{pmatrix}\begin{pmatrix}20\\ -3\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & 2\end{pmatrix} \to \begin{pmatrix}2 & 13\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}2 & 13\end{pmatrix}\begin{pmatrix}20\\ -3\end{pmatrix}$, c'est-à-dire : $20u - 3v = 1$, avec : $(u, v) = (2{,}13)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 20, et on a : $-3v \equiv 1 \bmod 20$. Ceci prouve que -3 admet pour inverse modulo 20 : $v = 13$. D'où le résultat.

Corrigé 66. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases}
59 = -4 \times (-14) + 3 & \left(\text{matriciellement : } \begin{pmatrix}59\\ -4\end{pmatrix} = \begin{pmatrix}-14 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-4\\ 3\end{pmatrix}\right)\\
-4 = 3 \times (-2) + 2 & \left(\text{matriciellement : } \begin{pmatrix}-4\\ 3\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 2\end{pmatrix}\right)\\
3 = 2 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 2\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}\right)\\
2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix}2\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 59 et -4 est 1, c'est-à-dire : -4 est inversible modulo 59. Déduisons-en aussi des entiers u et v tels que : $59u + -4v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 14\end{pmatrix}\begin{pmatrix}59\\ -4\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & -15\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & -15\end{pmatrix}\begin{pmatrix}59\\ -4\end{pmatrix}$, c'est-à-dire : $59u - 4v = 1$, avec : $(u, v) = (-1, -15)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 59, et on a : $-4v \equiv 1 \bmod 59$. Ceci prouve que -4 admet pour inverse modulo 59 : $v = -15$. D'où le résultat.

Corrigé 67. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 3

$$\begin{cases}
22 = 3 \times 7 + 1\\
3 = 1 \times 3 + 0
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 22 et 3 est 1, c'est-à-dire : 3 est inversible modulo 22. De plus la première division euclidienne implique immédiatement : $22u + 3v = 1$, avec : $(u, v) = (1, -7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 22, et on a : $3v \equiv 1 \bmod 22$. Ceci prouve que 3 admet pour inverse modulo 22 : $v = -7$. D'où le résultat.

Corrigé 68. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve ← page 3

alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement :

$$\begin{cases} 47 = 25\times 1+22 & \left(\text{matriciellement : } \begin{pmatrix}47\\25\end{pmatrix}=\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}25\\22\end{pmatrix}\right)\\ 25 = 22\times 1+3 & \left(\text{matriciellement : } \begin{pmatrix}25\\22\end{pmatrix}=\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}22\\3\end{pmatrix}\right)\\ 22 = 3\times 7+1 & \left(\text{matriciellement : } \begin{pmatrix}22\\3\end{pmatrix}=\begin{pmatrix}7&1\\1&0\end{pmatrix}\begin{pmatrix}3\\1\end{pmatrix}\right)\\ 3 = 1\times 3+0 & \left(\text{matriciellement : } \begin{pmatrix}3\\1\end{pmatrix}=\begin{pmatrix}3&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right)\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 47 et 25 est 1, c'est-à-dire : 25 est inversible modulo 47. Déduisons-en aussi des entiers u et v tels que : $47u+25v=1$. Les relations matricielles ci-dessus impliquent :

$$1=\begin{pmatrix}1&0\end{pmatrix}\begin{pmatrix}0&1\\1&-3\end{pmatrix}\begin{pmatrix}0&1\\1&-7\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}47\\25\end{pmatrix}$$
$$\searrow\quad\downarrow\qquad\downarrow\qquad\downarrow\qquad\downarrow$$
$$\begin{pmatrix}0&1\end{pmatrix}\to\begin{pmatrix}1&-7\end{pmatrix}\to\begin{pmatrix}-7&8\end{pmatrix}\to\begin{pmatrix}8&-15\end{pmatrix}$$

En résumé on a : $1=\begin{pmatrix}8&-15\end{pmatrix}\begin{pmatrix}47\\25\end{pmatrix}$, c'est-à-dire : $47u+25v=1$, avec : $(u,v)=(8,-15)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 47, et on a : $25v\equiv 1 \bmod 47$. Ceci prouve que 25 admet pour inverse modulo 47 : $v=-15$. D'où le résultat.

Corrigé 69. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases} 25 = 23\times 1+2 & \left(\text{matriciellement : } \begin{pmatrix}25\\23\end{pmatrix}=\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}23\\2\end{pmatrix}\right)\\ 23 = 2\times 11+1 & \left(\text{matriciellement : } \begin{pmatrix}23\\2\end{pmatrix}=\begin{pmatrix}11&1\\1&0\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix}\right)\\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix}2\\1\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right)\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 25 et 23 est 1, c'est-à-dire : 23 est inversible modulo 25. Déduisons-en aussi des entiers u et v tels que : $25u+23v=1$. Les relations matricielles ci-dessus impliquent :

$$1=\begin{pmatrix}1&0\end{pmatrix}\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&-11\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}25\\23\end{pmatrix}$$
$$\searrow\quad\downarrow\qquad\downarrow\qquad\downarrow$$
$$\begin{pmatrix}0&1\end{pmatrix}\to\begin{pmatrix}1&-11\end{pmatrix}\to\begin{pmatrix}-11&12\end{pmatrix}$$

En résumé on a : $1=\begin{pmatrix}-11&12\end{pmatrix}\begin{pmatrix}25\\23\end{pmatrix}$, c'est-à-dire : $25u+23v=1$, avec : $(u,v)=(-11,12)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 25, et on a : $23v\equiv 1 \bmod 25$. Ceci prouve que 23 admet pour inverse modulo 25 : $v=12$. D'où le résultat.

Corrigé 70. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu ← page 3

la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 17 = 3\times 5+2 & \left(\text{matriciellement : } \begin{pmatrix}17\\3\end{pmatrix} = \begin{pmatrix}5&1\\1&0\end{pmatrix}\begin{pmatrix}3\\2\end{pmatrix}\right) \\ 3 = 2\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix}3\\2\end{pmatrix} = \begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix}2\\1\end{pmatrix} = \begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 17 et 3 est 1, c'est-à-dire : 3 est inversible modulo 17. Déduisons-en aussi des entiers u et v tels que : $17u+3v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1&0\end{pmatrix}\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&-5\end{pmatrix}\begin{pmatrix}17\\3\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$
$$\begin{pmatrix}0&1\end{pmatrix} \to \begin{pmatrix}1&-1\end{pmatrix} \to \begin{pmatrix}-1&6\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1&6\end{pmatrix}\begin{pmatrix}17\\3\end{pmatrix}$, c'est-à-dire : $17u+3v=1$, avec : $(u,v)=(-1,6)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 17, et on a : $3v \equiv 1 \bmod 17$. Ceci prouve que 3 admet pour inverse modulo 17 : $v=6$. D'où le résultat.

Corrigé 71. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases} 53 = 3\times 17+2 & \left(\text{matriciellement : } \begin{pmatrix}53\\3\end{pmatrix} = \begin{pmatrix}17&1\\1&0\end{pmatrix}\begin{pmatrix}3\\2\end{pmatrix}\right) \\ 3 = 2\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix}3\\2\end{pmatrix} = \begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix}2\\1\end{pmatrix} = \begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 53 et 3 est 1, c'est-à-dire : 3 est inversible modulo 53. Déduisons-en aussi des entiers u et v tels que : $53u+3v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1&0\end{pmatrix}\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&-17\end{pmatrix}\begin{pmatrix}53\\3\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$
$$\begin{pmatrix}0&1\end{pmatrix} \to \begin{pmatrix}1&-1\end{pmatrix} \to \begin{pmatrix}-1&18\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1&18\end{pmatrix}\begin{pmatrix}53\\3\end{pmatrix}$, c'est-à-dire : $53u+3v=1$, avec : $(u,v)=(-1,18)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 53, et on a : $3v \equiv 1 \bmod 53$. Ceci prouve que 3 admet pour inverse modulo 53 : $v=18$. D'où le résultat.

Corrigé 72. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On ← page 3

trouve successivement :

$$\begin{cases} 22 = 15\times 1+7 & \left(\text{matriciellement : } \begin{pmatrix}22\\15\end{pmatrix}=\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}15\\7\end{pmatrix}\right)\\ 15 = 7\times 2+1 & \left(\text{matriciellement : } \begin{pmatrix}15\\7\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}7\\1\end{pmatrix}\right)\\ 7 = 1\times 7+0 & \left(\text{matriciellement : } \begin{pmatrix}7\\1\end{pmatrix}=\begin{pmatrix}7&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right)\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 22 et 15 est 1, c'est-à-dire : 15 est inversible modulo 22. Déduisons-en aussi des entiers u et v tels que : $22u+15v=1$. Les relations matricielles ci-dessus impliquent :

$$1=\begin{pmatrix}1&0\end{pmatrix}\begin{pmatrix}0&1\\1&-7\end{pmatrix}\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&-1\end{pmatrix}\begin{pmatrix}22\\15\end{pmatrix}$$
$$\searrow\quad\downarrow\qquad\qquad\downarrow\qquad\qquad\downarrow$$
$$\begin{pmatrix}0&1\end{pmatrix}\to\begin{pmatrix}1&-2\end{pmatrix}\to\begin{pmatrix}-2&3\end{pmatrix}$$

En résumé on a : $1=\begin{pmatrix}-2&3\end{pmatrix}\begin{pmatrix}22\\15\end{pmatrix}$, c'est-à-dire : $22u+15v=1$, avec : $(u,v)=(-2,3)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 22, et on a : $15v\equiv 1 \bmod 22$. Ceci prouve que 15 admet pour inverse modulo 22 : $v=3$. D'où le résultat.

Corrigé 73. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 3

$$\begin{cases} 23 = -7\times(-3)+2 & \left(\text{matriciellement : } \begin{pmatrix}23\\-7\end{pmatrix}=\begin{pmatrix}-3&1\\1&0\end{pmatrix}\begin{pmatrix}-7\\2\end{pmatrix}\right)\\ -7 = 2\times(-4)+1 & \left(\text{matriciellement : } \begin{pmatrix}-7\\2\end{pmatrix}=\begin{pmatrix}-4&1\\1&0\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix}\right)\\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix}2\\1\end{pmatrix}=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right)\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 23 et -7 est 1, c'est-à-dire : -7 est inversible modulo 23. Déduisons-en aussi des entiers u et v tels que : $23u+-7v=1$. Les relations matricielles ci-dessus impliquent :

$$1=\begin{pmatrix}1&0\end{pmatrix}\begin{pmatrix}0&1\\1&-2\end{pmatrix}\begin{pmatrix}0&1\\1&4\end{pmatrix}\begin{pmatrix}0&1\\1&3\end{pmatrix}\begin{pmatrix}23\\-7\end{pmatrix}$$
$$\searrow\quad\downarrow\qquad\qquad\downarrow\qquad\qquad\downarrow$$
$$\begin{pmatrix}0&1\end{pmatrix}\to\begin{pmatrix}1&4\end{pmatrix}\to\begin{pmatrix}4&13\end{pmatrix}$$

En résumé on a : $1=\begin{pmatrix}4&13\end{pmatrix}\begin{pmatrix}23\\-7\end{pmatrix}$, c'est-à-dire : $23u-7v=1$, avec : $(u,v)=(4,13)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 23, et on a : $-7v\equiv 1 \bmod 23$. Ceci prouve que -7 admet pour inverse modulo 23 : $v=13$. D'où le résultat.

Corrigé 74. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On ← page 3

trouve successivement :

$$\begin{cases} 192 = 5\times 38+2 & \left(\text{matriciellement : } \begin{pmatrix} 192 \\ 5 \end{pmatrix} = \begin{pmatrix} 38 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 \\ 2 \end{pmatrix}\right) \\ 5 = 2\times 2+1 & \left(\text{matriciellement : } \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 192 et 5 est 1, c'est-à-dire : 5 est inversible modulo 192. Déduisons-en aussi des entiers u et v tels que : $192u+5v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -38 \end{pmatrix}\begin{pmatrix} 192 \\ 5 \end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -2 \end{pmatrix} \to \begin{pmatrix} -2 & 77 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -2 & 77 \end{pmatrix}\begin{pmatrix} 192 \\ 5 \end{pmatrix}$, c'est-à-dire : $192u+5v=1$, avec : $(u,v)=(-2,77)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 192, et on a : $5v \equiv 1 \bmod 192$. Ceci prouve que 5 admet pour inverse modulo 192 : $v=77$. D'où le résultat.

Corrigé 75. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 3

$$\begin{cases} 21 = 10\times 2+1 \\ 10 = 1\times 10+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 21 et 10 est 1, c'est-à-dire : 10 est inversible modulo 21. De plus la première division euclidienne implique immédiatement : $21u+10v=1$, avec : $(u,v)=(1,-2)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 21, et on a : $10v \equiv 1 \bmod 21$. Ceci prouve que 10 admet pour inverse modulo 21 : $v=-2$. D'où le résultat.

Corrigé 76. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 3

$$\begin{cases} 18 = -5\times(-3)+3 & \left(\text{matriciellement : } \begin{pmatrix} 18 \\ -5 \end{pmatrix} = \begin{pmatrix} -3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -5 \\ 3 \end{pmatrix}\right) \\ -5 = 3\times(-2)+1 & \left(\text{matriciellement : } \begin{pmatrix} -5 \\ 3 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 1 \end{pmatrix}\right) \\ 3 = 1\times 3+0 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 18 et -5 est 1, c'est-à-dire : -5 est inversible modulo 18. Déduisons-en aussi des entiers u et v tels que : $18u+-5v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 18 \\ -5 \end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 7 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} 2 & 7 \end{pmatrix} \begin{pmatrix} 18 \\ -5 \end{pmatrix}$, c'est-à-dire : $18u - 5v = 1$, avec : $(u, v) = (2{,}7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 18, et on a : $-5v \equiv 1 \bmod 18$. Ceci prouve que -5 admet pour inverse modulo 18 : $v = 7$. D'où le résultat.

Corrigé 77. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 3

$$\begin{cases} 139 = -7 \times (-19) + 6 & \left(\text{matriciellement : } \begin{pmatrix} 139 \\ -7 \end{pmatrix} = \begin{pmatrix} -19 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -7 \\ 6 \end{pmatrix} \right) \\ -7 = 6 \times (-2) + 5 & \left(\text{matriciellement : } \begin{pmatrix} -7 \\ 6 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 6 \\ 5 \end{pmatrix} \right) \\ 6 = 5 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix} 6 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 5 \\ 1 \end{pmatrix} \right) \\ 5 = 1 \times 5 + 0 & \left(\text{matriciellement : } \begin{pmatrix} 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 139 et -7 est 1, c'est-à-dire : -7 est inversible modulo 139. Déduisons-en aussi des entiers u et v tels que : $139u + -7v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 19 \end{pmatrix} \begin{pmatrix} 139 \\ -7 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & -20 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -1 & -20 \end{pmatrix} \begin{pmatrix} 139 \\ -7 \end{pmatrix}$, c'est-à-dire : $139u - 7v = 1$, avec : $(u, v) = (-1, -20)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 139, et on a : $-7v \equiv 1 \bmod 139$. Ceci prouve que -7 admet pour inverse modulo 139 : $v = -20$. D'où le résultat.

Corrigé 78. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases} 17 = 4 \times 4 + 1 \\ 4 = 1 \times 4 + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 17 et 4 est 1, c'est-à-dire : 4 est inversible modulo 17. De plus la première division euclidienne implique immédiatement : $17u + 4v = 1$, avec : $(u, v) = (1, -4)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 17, et on a : $4v \equiv 1 \bmod 17$. Ceci prouve que 4 admet pour inverse modulo 17 : $v = -4$. D'où le résultat.

Corrigé 79. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases} 22 = -3 \times (-7) + 1 \\ -3 = 1 \times (-3) + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 22 et -3 est 1, c'est-à-dire : -3 est inversible modulo 22. De plus la première division euclidienne implique immédiatement : $22u - 3v = 1$, avec :

$(u, v) = (1,7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 22, et on a : $-3v \equiv 1 \bmod 22$. Ceci prouve que -3 admet pour inverse modulo 22 : $v = 7$. D'où le résultat.

Corrigé 80. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases} 19 = -15 \times (-1) + 4 & \left(\text{matriciellement : } \begin{pmatrix} 19 \\ -15 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -15 \\ 4 \end{pmatrix} \right) \\ -15 = 4 \times (-4) + 1 & \left(\text{matriciellement : } \begin{pmatrix} -15 \\ 4 \end{pmatrix} = \begin{pmatrix} -4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 \\ 1 \end{pmatrix} \right) \\ 4 = 1 \times 4 + 0 & \left(\text{matriciellement : } \begin{pmatrix} 4 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 19 et -15 est 1, c'est-à-dire : -15 est inversible modulo 19. Déduisons-en aussi des entiers u et v tels que : $19u + -15v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 19 \\ -15 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 4 \end{pmatrix} \to \begin{pmatrix} 4 & 5 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} 4 & 5 \end{pmatrix} \begin{pmatrix} 19 \\ -15 \end{pmatrix}$, c'est-à-dire : $19u - 15v = 1$, avec : $(u, v) = (4,5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 19, et on a : $-15v \equiv 1 \bmod 19$. Ceci prouve que -15 admet pour inverse modulo 19 : $v = 5$. D'où le résultat.

Corrigé 81. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases} 32 = -7 \times (-4) + 4 & \left(\text{matriciellement : } \begin{pmatrix} 32 \\ -7 \end{pmatrix} = \begin{pmatrix} -4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -7 \\ 4 \end{pmatrix} \right) \\ -7 = 4 \times (-2) + 1 & \left(\text{matriciellement : } \begin{pmatrix} -7 \\ 4 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 \\ 1 \end{pmatrix} \right) \\ 4 = 1 \times 4 + 0 & \left(\text{matriciellement : } \begin{pmatrix} 4 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 32 et -7 est 1, c'est-à-dire : -7 est inversible modulo 32. Déduisons-en aussi des entiers u et v tels que : $32u + -7v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 32 \\ -7 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 9 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} 2 & 9 \end{pmatrix} \begin{pmatrix} 32 \\ -7 \end{pmatrix}$, c'est-à-dire : $32u - 7v = 1$, avec : $(u, v) = (2,9)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 32, et on a : $-7v \equiv 1 \bmod 32$. Ceci prouve que -7 admet pour inverse modulo 32 : $v = 9$. D'où le résultat.

Corrigé 82. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases} 22 = -9\times(-2)+4 & \left(\text{matriciellement : } \begin{pmatrix} 22 \\ -9 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -9 \\ 4 \end{pmatrix}\right) \\ -9 = 4\times(-3)+3 & \left(\text{matriciellement : } \begin{pmatrix} -9 \\ 4 \end{pmatrix} = \begin{pmatrix} -3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 4 \\ 3 \end{pmatrix}\right) \\ 4 = 3\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 1 \end{pmatrix}\right) \\ 3 = 1\times 3+0 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 22 et -9 est 1, c'est-à-dire : -9 est inversible modulo 22. Déduisons-en aussi des entiers u et v tels que : $22u+-9v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 22 \\ -9 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & -2 \end{pmatrix} \to \begin{pmatrix} -2 & -5 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -2 & -5 \end{pmatrix}\begin{pmatrix} 22 \\ -9 \end{pmatrix}$, c'est-à-dire : $22u-9v=1$, avec : $(u,v)=(-2,-5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 22, et on a : $-9v \equiv 1 \bmod 22$. Ceci prouve que -9 admet pour inverse modulo 22 : $v=-5$. D'où le résultat.

Corrigé 83. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 4

$$\begin{cases} 116 = 49\times 2+18 & \left(\text{matriciellement : } \begin{pmatrix} 116 \\ 49 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 49 \\ 18 \end{pmatrix}\right) \\ 49 = 18\times 2+13 & \left(\text{matriciellement : } \begin{pmatrix} 49 \\ 18 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 18 \\ 13 \end{pmatrix}\right) \\ 18 = 13\times 1+5 & \left(\text{matriciellement : } \begin{pmatrix} 18 \\ 13 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 13 \\ 5 \end{pmatrix}\right) \\ 13 = 5\times 2+3 & \left(\text{matriciellement : } \begin{pmatrix} 13 \\ 5 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 \\ 3 \end{pmatrix}\right) \\ 5 = 3\times 1+2 & \left(\text{matriciellement : } \begin{pmatrix} 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}\right) \\ 3 = 2\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 116 et 49 est 1, c'est-à-dire : 49 est inversible modulo 116. Déduisons-en aussi des entiers u et v tels que : $116u+49v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}116\\ 49\end{pmatrix}$$

$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & 2\end{pmatrix} \to \begin{pmatrix}2 & -5\end{pmatrix} \to \begin{pmatrix}-5 & 7\end{pmatrix} \to \begin{pmatrix}7 & -19\end{pmatrix} \to \begin{pmatrix}-19 & 45\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-19 & 45\end{pmatrix}\begin{pmatrix}116\\ 49\end{pmatrix}$, c'est-à-dire : $116u + 49v = 1$, avec : $(u, v) = (-19{,}45)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 116, et on a : $49v \equiv 1 \bmod 116$. Ceci prouve que 49 admet pour inverse modulo 116 : $v = 45$. D'où le résultat.

Corrigé 84. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases} 19 &= 6 \times 3 + 1 \\ 6 &= 1 \times 6 + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 19 et 6 est 1, c'est-à-dire : 6 est inversible modulo 19. De plus la première division euclidienne implique immédiatement : $19u + 6v = 1$, avec : $(u, v) = (1, -3)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 19, et on a : $6v \equiv 1 \bmod 19$. Ceci prouve que 6 admet pour inverse modulo 19 : $v = -3$. D'où le résultat.

Corrigé 85. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases} 37 &= 6 \times 6 + 1 \\ 6 &= 1 \times 6 + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 37 et 6 est 1, c'est-à-dire : 6 est inversible modulo 37. De plus la première division euclidienne implique immédiatement : $37u + 6v = 1$, avec : $(u, v) = (1, -6)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 37, et on a : $6v \equiv 1 \bmod 37$. Ceci prouve que 6 admet pour inverse modulo 37 : $v = -6$. D'où le résultat.

Corrigé 86. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 4

$$\begin{cases} 101 &= 31 \times 3 + 8 & \left(\text{matriciellement : } \begin{pmatrix}101\\ 31\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}31\\ 8\end{pmatrix}\right) \\ 31 &= 8 \times 3 + 7 & \left(\text{matriciellement : } \begin{pmatrix}31\\ 8\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}8\\ 7\end{pmatrix}\right) \\ 8 &= 7 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}8\\ 7\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}7\\ 1\end{pmatrix}\right) \\ 7 &= 1 \times 7 + 0 & \left(\text{matriciellement : } \begin{pmatrix}7\\ 1\end{pmatrix} = \begin{pmatrix}7 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 101 et 31 est 1, c'est-à-dire : 31 est inversible modulo 101. Déduisons-en aussi des entiers u et v tels que : $101u + 31v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -7\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}101\\ 31\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & 4\end{pmatrix} \to \begin{pmatrix}4 & -13\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}4 & -13\end{pmatrix}\begin{pmatrix}101\\ 31\end{pmatrix}$, c'est-à-dire : $101u + 31v = 1$, avec : $(u, v) = (4, -13)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 101, et on a : $31v \equiv 1 \bmod 101$. Ceci prouve que 31 admet pour inverse modulo 101 : $v = -13$. D'où le résultat.

Corrigé 87. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 4

$$\begin{cases} 80 = 3 \times 26 + 2 & \left(\text{matriciellement : } \begin{pmatrix}80\\ 3\end{pmatrix} = \begin{pmatrix}26 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 2\end{pmatrix}\right) \\ 3 = 2 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 2\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}\right) \\ 2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix}2\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 80 et 3 est 1, c'est-à-dire : 3 est inversible modulo 80. Déduisons-en aussi des entiers u et v tels que : $80u + 3v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -26\end{pmatrix}\begin{pmatrix}80\\ 3\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & 27\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & 27\end{pmatrix}\begin{pmatrix}80\\ 3\end{pmatrix}$, c'est-à-dire : $80u + 3v = 1$, avec : $(u, v) = (-1{,}27)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 80, et on a : $3v \equiv 1 \bmod 80$. Ceci prouve que 3 admet pour inverse modulo 80 : $v = 27$. D'où le résultat.

Corrigé 88. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases} 35 = 9 \times 3 + 8 & \left(\text{matriciellement : } \begin{pmatrix}35\\ 9\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}9\\ 8\end{pmatrix}\right) \\ 9 = 8 \times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}9\\ 8\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}8\\ 1\end{pmatrix}\right) \\ 8 = 1 \times 8 + 0 & \left(\text{matriciellement : } \begin{pmatrix}8\\ 1\end{pmatrix} = \begin{pmatrix}8 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 35 et 9 est 1, c'est-à-dire : 9 est inversible modulo 35. Déduisons-en aussi des entiers u et v tels que : $35u + 9v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -8\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}35\\ 9\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & 4\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -1 & 4 \end{pmatrix} \begin{pmatrix} 35 \\ 9 \end{pmatrix}$, c'est-à-dire : $35u+9v = 1$, avec : $(u, v) = (-1,4)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 35, et on a : $9v \equiv 1 \bmod 35$. Ceci prouve que 9 admet pour inverse modulo 35 : $v = 4$. D'où le résultat.

Corrigé 89. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 4

$$\begin{cases} 499 &= 3 \times 166 + 1 \\ 3 &= 1 \times 3 + 0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 499 et 3 est 1, c'est-à-dire : 3 est inversible modulo 499. De plus la première division euclidienne implique immédiatement : $499u + 3v = 1$, avec : $(u, v) = (1, -166)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 499, et on a : $3v \equiv 1 \bmod 499$. Ceci prouve que 3 admet pour inverse modulo 499 : $v = -166$. D'où le résultat.

Corrigé 90. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 4

$$\begin{cases} 199 &= -52 \times (-3) + 43 & \left(\text{matriciellement : } \begin{pmatrix} 199 \\ -52 \end{pmatrix} = \begin{pmatrix} -3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -52 \\ 43 \end{pmatrix}\right) \\ -52 &= 43 \times (-2) + 34 & \left(\text{matriciellement : } \begin{pmatrix} -52 \\ 43 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 43 \\ 34 \end{pmatrix}\right) \\ 43 &= 34 \times 1 + 9 & \left(\text{matriciellement : } \begin{pmatrix} 43 \\ 34 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 34 \\ 9 \end{pmatrix}\right) \\ 34 &= 9 \times 3 + 7 & \left(\text{matriciellement : } \begin{pmatrix} 34 \\ 9 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 9 \\ 7 \end{pmatrix}\right) \\ 9 &= 7 \times 1 + 2 & \left(\text{matriciellement : } \begin{pmatrix} 9 \\ 7 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 7 \\ 2 \end{pmatrix}\right) \\ 7 &= 2 \times 3 + 1 & \left(\text{matriciellement : } \begin{pmatrix} 7 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 &= 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 199 et -52 est 1, c'est-à-dire : -52 est inversible modulo 199. Déduisons-en aussi des entiers u et v tels que : $199u + -52v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 199 \\ -52 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -3 \end{pmatrix} \to \begin{pmatrix} -3 & 4 \end{pmatrix} \to \begin{pmatrix} 4 & -15 \end{pmatrix} \to \begin{pmatrix} -15 & 19 \end{pmatrix} \to \begin{pmatrix} 19 & 23 \end{pmatrix} \to \begin{pmatrix} 23 & 88 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} 23 & 88 \end{pmatrix} \begin{pmatrix} 199 \\ -52 \end{pmatrix}$, c'est-à-dire : $199u - 52v = 1$, avec : $(u, v) = (23,88)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 199, et on a : $-52v \equiv 1 \bmod 199$. Ceci prouve que -52 admet pour inverse modulo 199 : $v = 88$. D'où le résultat.

Corrigé 91. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour ← page 4

s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 19 &= -9\times(-2)+1 \\ -9 &= 1\times(-9)+0 \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 19 et -9 est 1, c'est-à-dire : -9 est inversible modulo 19. De plus la première division euclidienne implique immédiatement : $19u-9v=1$, avec : $(u,v)=(1{,}2)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 19, et on a : $-9v\equiv 1 \bmod 19$. Ceci prouve que -9 admet pour inverse modulo 19 : $v=2$. D'où le résultat.

Corrigé 92. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 4

$$\begin{cases} 59 &= 8\times 7+3 & \left(\text{matriciellement : } \begin{pmatrix} 59 \\ 8 \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 8 \\ 3 \end{pmatrix}\right) \\ 8 &= 3\times 2+2 & \left(\text{matriciellement : } \begin{pmatrix} 8 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}\right) \\ 3 &= 2\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}\right) \\ 2 &= 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 59 et 8 est 1, c'est-à-dire : 8 est inversible modulo 59. Déduisons-en aussi des entiers u et v tels que : $59u+8v=1$. Les relations matricielles ci-dessus impliquent :

$$1=\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -7 \end{pmatrix}\begin{pmatrix}59\\8\end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & 3 \end{pmatrix} \to \begin{pmatrix} 3 & -22 \end{pmatrix}$$

En résumé on a : $1=\begin{pmatrix} 3 & -22 \end{pmatrix}\begin{pmatrix}59\\8\end{pmatrix}$, c'est-à-dire : $59u+8v=1$, avec : $(u,v)=(3,-22)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 59, et on a : $8v\equiv 1 \bmod 59$. Ceci prouve que 8 admet pour inverse modulo 59 : $v=-22$. D'où le résultat.

Corrigé 93. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases} 23 &= 4\times 5+3 & \left(\text{matriciellement : } \begin{pmatrix} 23 \\ 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 4 \\ 3 \end{pmatrix}\right) \\ 4 &= 3\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 1 \end{pmatrix}\right) \\ 3 &= 1\times 3+0 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 23 et 4 est 1, c'est-à-dire : 4 est inversible modulo 23. Déduisons-en aussi des entiers u et v tels que : $23u+4v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -5\end{pmatrix}\begin{pmatrix}23\\ 4\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & 6\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & 6\end{pmatrix}\begin{pmatrix}23\\ 4\end{pmatrix}$, c'est-à-dire : $23u+4v=1$, avec : $(u,v)=(-1{,}6)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 23, et on a : $4v \equiv 1 \bmod 23$. Ceci prouve que 4 admet pour inverse modulo 23 : $v = 6$. D'où le résultat.

Corrigé 94. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 4

$$\begin{cases}
103157 = 25\times 4126 + 7 & \left(\text{matriciellement : } \begin{pmatrix}103157\\ 25\end{pmatrix} = \begin{pmatrix}4126 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}25\\ 7\end{pmatrix}\right)\\
25 = 7\times 3 + 4 & \left(\text{matriciellement : } \begin{pmatrix}25\\ 7\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}7\\ 4\end{pmatrix}\right)\\
7 = 4\times 1 + 3 & \left(\text{matriciellement : } \begin{pmatrix}7\\ 4\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}4\\ 3\end{pmatrix}\right)\\
4 = 3\times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}4\\ 3\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 1\end{pmatrix}\right)\\
3 = 1\times 3 + 0 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 1\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 103157 et 25 est 1, c'est-à-dire : 25 est inversible modulo 103157. Déduisons-en aussi des entiers u et v tels que : $103157u+25v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -4126\end{pmatrix}\begin{pmatrix}103157\\ 25\end{pmatrix}$$
$$\searrow \quad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -1\end{pmatrix} \to \begin{pmatrix}-1 & 2\end{pmatrix} \to \begin{pmatrix}2 & -7\end{pmatrix} \to \begin{pmatrix}-7 & 28884\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-7 & 28884\end{pmatrix}\begin{pmatrix}103157\\ 25\end{pmatrix}$, c'est-à-dire : $103157u+25v=1$, avec : $(u,v)=(-7{,}28884)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 103157, et on a : $25v \equiv 1 \bmod 103157$. Ceci prouve que 25 admet pour inverse modulo 103157 : $v = 28884$. D'où le résultat.

Corrigé 95. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases}
19 = 4\times 4 + 3 & \left(\text{matriciellement : } \begin{pmatrix}19\\ 4\end{pmatrix} = \begin{pmatrix}4 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}4\\ 3\end{pmatrix}\right)\\
4 = 3\times 1 + 1 & \left(\text{matriciellement : } \begin{pmatrix}4\\ 3\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}3\\ 1\end{pmatrix}\right)\\
3 = 1\times 3 + 0 & \left(\text{matriciellement : } \begin{pmatrix}3\\ 1\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 19 et 4 est 1, c'est-à-dire : 4 est inversible modulo 19. Déduisons-en aussi des entiers u et v tels que : $19u+4v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -4\end{pmatrix}\begin{pmatrix}19\\ 4\end{pmatrix}$$
$$\searrow\quad\downarrow\qquad\qquad\downarrow\qquad\qquad\downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix}\to\begin{pmatrix}1 & -1\end{pmatrix}\to\begin{pmatrix}-1 & 5\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-1 & 5\end{pmatrix}\begin{pmatrix}19\\ 4\end{pmatrix}$, c'est-à-dire : $19u+4v=1$, avec : $(u,v)=(-1{,}5)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 19, et on a : $4v \equiv 1 \bmod 19$. Ceci prouve que 4 admet pour inverse modulo 19 : $v = 5$. D'où le résultat.

Corrigé 96. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases}
17 = 12\times 1+5 & \left(\text{matriciellement : } \begin{pmatrix}17\\12\end{pmatrix} = \begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}12\\5\end{pmatrix}\right)\\
12 = 5\times 2+2 & \left(\text{matriciellement : } \begin{pmatrix}12\\5\end{pmatrix} = \begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}5\\2\end{pmatrix}\right)\\
5 = 2\times 2+1 & \left(\text{matriciellement : } \begin{pmatrix}5\\2\end{pmatrix} = \begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix}\right)\\
2 = 1\times 2+0 & \left(\text{matriciellement : } \begin{pmatrix}2\\1\end{pmatrix} = \begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 17 et 12 est 1, c'est-à-dire : 12 est inversible modulo 17. Déduisons-en aussi des entiers u et v tels que : $17u+12v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}17\\ 12\end{pmatrix}$$
$$\searrow\quad\downarrow\qquad\qquad\downarrow\qquad\qquad\downarrow\qquad\qquad\downarrow$$
$$\begin{pmatrix}0 & 1\end{pmatrix}\to\begin{pmatrix}1 & -2\end{pmatrix}\to\begin{pmatrix}-2 & 5\end{pmatrix}\to\begin{pmatrix}5 & -7\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}5 & -7\end{pmatrix}\begin{pmatrix}17\\12\end{pmatrix}$, c'est-à-dire : $17u+12v=1$, avec : $(u,v)=(5,-7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 17, et on a : $12v \equiv 1 \bmod 17$. Ceci prouve que 12 admet pour inverse modulo 17 : $v = -7$. D'où le résultat.

Corrigé 97. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases}
38 = -21\times(-1)+17 & \left(\text{matriciellement : } \begin{pmatrix}38\\-21\end{pmatrix} = \begin{pmatrix}-1&1\\1&0\end{pmatrix}\begin{pmatrix}-21\\17\end{pmatrix}\right)\\
-21 = 17\times(-2)+13 & \left(\text{matriciellement : } \begin{pmatrix}-21\\17\end{pmatrix} = \begin{pmatrix}-2&1\\1&0\end{pmatrix}\begin{pmatrix}17\\13\end{pmatrix}\right)\\
17 = 13\times 1+4 & \left(\text{matriciellement : } \begin{pmatrix}17\\13\end{pmatrix} = \begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}13\\4\end{pmatrix}\right)\\
13 = 4\times 3+1 & \left(\text{matriciellement : } \begin{pmatrix}13\\4\end{pmatrix} = \begin{pmatrix}3&1\\1&0\end{pmatrix}\begin{pmatrix}4\\1\end{pmatrix}\right)\\
4 = 1\times 4+0 & \left(\text{matriciellement : } \begin{pmatrix}4\\1\end{pmatrix} = \begin{pmatrix}4&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 38 et -21 est 1, c'est-à-dire : -21 est inversible modulo 38. Déduisons-en aussi des entiers u et v tels que : $38u + -21v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -4\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}38\\ -21\end{pmatrix}$$

$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -3\end{pmatrix} \to \begin{pmatrix}-3 & 4\end{pmatrix} \to \begin{pmatrix}4 & 5\end{pmatrix} \to \begin{pmatrix}5 & 9\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}5 & 9\end{pmatrix}\begin{pmatrix}38\\ -21\end{pmatrix}$, c'est-à-dire : $38u - 21v = 1$, avec : $(u, v) = (5{,}9)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 38, et on a : $-21v \equiv 1 \bmod 38$. Ceci prouve que -21 admet pour inverse modulo 38 : $v = 9$. D'où le résultat.

Corrigé 98. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement : ← page 4

$$\begin{cases}
19 = -12 \times (-1) + 7 & \left(\text{matriciellement : } \begin{pmatrix}19\\ -12\end{pmatrix} = \begin{pmatrix}-1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-12\\ 7\end{pmatrix}\right)\\
-12 = 7 \times (-2) + 2 & \left(\text{matriciellement : } \begin{pmatrix}-12\\ 7\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}7\\ 2\end{pmatrix}\right)\\
7 = 2 \times 3 + 1 & \left(\text{matriciellement : } \begin{pmatrix}7\\ 2\end{pmatrix} = \begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}2\\ 1\end{pmatrix}\right)\\
2 = 1 \times 2 + 0 & \left(\text{matriciellement : } \begin{pmatrix}2\\ 1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\right)
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 19 et -12 est 1, c'est-à-dire : -12 est inversible modulo 19. Déduisons-en aussi des entiers u et v tels que : $19u + -12v = 1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -3\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}19\\ -12\end{pmatrix}$$

$$\begin{pmatrix}0 & 1\end{pmatrix} \to \begin{pmatrix}1 & -3\end{pmatrix} \to \begin{pmatrix}-3 & -5\end{pmatrix} \to \begin{pmatrix}-5 & -8\end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix}-5 & -8\end{pmatrix}\begin{pmatrix}19\\ -12\end{pmatrix}$, c'est-à-dire : $19u - 12v = 1$, avec : $(u, v) = (-5, -8)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 19, et on a : $-12v \equiv 1 \bmod 19$. Ceci prouve que -12 admet pour inverse modulo 19 : $v = -8$. D'où le résultat.

Corrigé 99. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide étendu. On trouve successivement : ← page 4

$$\begin{cases}
125 = -4 \times (-31) + 1\\
-4 = 1 \times (-4) + 0
\end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 125 et -4 est 1, c'est-à-dire : -4 est inversible modulo 125. De plus la première division euclidienne implique immédiatement : $125u - 4v = 1$, avec : $(u, v) = (1{,}31)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 125, et on a : $-4v \equiv 1 \bmod 125$. Ceci prouve que -4 admet pour inverse modulo 125 : $v = 31$. D'où le résultat.

Corrigé 100. On sait qu'un élément est inversible modulo n si et seulement s'il est premier avec n, et qu'on trouve alors son inverse grâce à une relation de Bézout. Nous y parviendrons grâce à l'algorithme d'Euclide ← page 4

étendu (vu la taille des entiers, on pourrait éventuellement trouver un inverse à l'œil nu ou rapidement à tâtons ; mais pour s'exercer à la pratique de l'algorithme je prétendrai que je n'ai rien vu). On trouve successivement :

$$\begin{cases} 27 = 4\times 6+3 & \left(\text{matriciellement : } \begin{pmatrix} 27 \\ 4 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 4 \\ 3 \end{pmatrix}\right) \\ 4 = 3\times 1+1 & \left(\text{matriciellement : } \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 \\ 1 \end{pmatrix}\right) \\ 3 = 1\times 3+0 & \left(\text{matriciellement : } \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \end{cases}$$

Le dernier reste non nul est 1. On en déduit que le plus grand commun diviseur de 27 et 4 est 1, c'est-à-dire : 4 est inversible modulo 27. Déduisons-en aussi des entiers u et v tels que : $27u+4v=1$. Les relations matricielles ci-dessus impliquent :

$$1 = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix}\begin{pmatrix} 27 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 \end{pmatrix} \to \begin{pmatrix} -1 & 7 \end{pmatrix}$$

En résumé on a : $1 = \begin{pmatrix} -1 & 7 \end{pmatrix}\begin{pmatrix} 27 \\ 4 \end{pmatrix}$, c'est-à-dire : $27u+4v=1$, avec : $(u,v)=(-1,7)$. On a trouvé une relation de Bézout. On réduit cette égalité modulo 27, et on a : $4v \equiv 1 \bmod 27$. Ceci prouve que 4 admet pour inverse modulo 27 : $v=7$. D'où le résultat.