Exercice 4 (Algorithme d'Euclide (suite)).

Pour tout couple d'entiers $a \in \mathbb{Z}$ et $b \in \mathbb{N}$, le théorème de Bézout établit l'existence d'un couple $(u, v) \in \mathbb{Z}^2$ d'entiers tel que $au + bv = \text{pgcd}(a, b)$.

L'algorithme de la Figure 1, appelé **algorithme d'Euclide étendu**, donne une méthode pratique pour calculer un tel couple.

Dans cet algorithme, les variables notées avec un indice s permettent de stocker en permanence l'état courant et l'état suivant (indice s) des trois variables `d`, `u` et `v`.

Généralement, pour comprendre le fonctionnement de cet algorithme, on utilise un tableau de suivi de variables. Voici par exemple le tableau de suivi de variables pour les valeurs d'entrée $a = 61$ et $b = 9$:

Itération	d	d_s	q	r	u	v	u_s	v_s
Init.	61	9	non défini	non défini	1	0	0	1
Fin itération 1	9	7	6	7	0	1	1	-6
Fin itération 2	7	2	1	2	1	-6	-1	7
Fin itération 3	2	1	3	1	-1	7	4	-27
Fin itération 4	1	$\boxed{0}$	2	0	$\boxed{4}$	$\boxed{-27}$	peu importe	peu importe
Fin de la boucle								

Sur cet exemple, on vérifie donc que l'algorithme fonctionne correctement car on trouve bien que la dernière valeur prise par `d` est 1, ce qui correspond bien au PGCD de 61 et de 9. De plus, on a bien

$$1 = 4 \times 61 + (-27) \times 9$$

$u = 4$ et $v = -27$ sont donc bien des entiers de Bézout valides dans ce cas.

1. Appliquer cet algorithme aux entiers $a = 63$ et $b = 11$ en remplissant un tableau de suivi de variables comme ci-dessous. Conclure pour cet exemple.

2. Écrire une fonction C

```
int euclide_etendu(int a, int b, int *u, int *v)
```

qui reçoit deux paramètres entiers `a` et `b` et qui calcule les entiers u, v, d. On respectera soigneusement le prototype imposé.

3. Justifier la *terminaison* de cette fonction.

4. Montrer que la propriété suivante est un *invariant de boucle.*

$$\mathcal{P} : \quad au + bv = d$$

Vous pouvez introduire toutes les notations qui vous semblent nécessaires.
On pourra commencer par le vérifier sur un exemple, en annotant **proprement** et de façon lisible le tableau de la première question.

5. En déduire la *correction* de votre fonction.

6. Démontrer le théorème de Bézout

Algorithme 1 : `euclide_etendu`

Donnée : a, `entier`
Donnée : b, `entier`

Variable de travail : d, `entier`
Variable de travail : u, `entier`
Variable de travail : v, `entier`

Variable de travail : tmp_u, `entier`
Variable de travail : tmp_v, `entier`

Variable de travail : d_s, `entier`
Variable de travail : u_s, `entier`
Variable de travail : v_s, `entier`

Variable de travail : r, `entier`
Variable de travail : q, `entier`

$d \leftarrow a$
$u \leftarrow 1$
$v \leftarrow 0$

$d_s \leftarrow b$
$u_s \leftarrow 0$
$v_s \leftarrow 1$

tant que $d_s \neq 0$ *faire*
    $(q, r) \leftarrow$ (quotient, reste) de la division euclidienne de d par d_s
    $tmp_u \leftarrow u_s$
    $tmp_v \leftarrow v_s$
    $u_s \leftarrow u - q \times u_s$
    $v_s \leftarrow v - q \times v_s$
    $u \leftarrow tmp_u$
    $v \leftarrow tmp_v$
    $d \leftarrow d_s$
    $d_s \leftarrow r$

Renvoyer les valeurs d, u et v.

FIGURE 1 – Algorithme d'Euclide étendu écrit en pseudo-code.