Algorithme d'Euclide

L'algorithme d'Euclide est basé sur le principe suivant :

Si $b|a$ alors pgcd(a,b) = b sinon pgcd(a,b) = pgcd(b,$a \mod b$).

Proposition 1. *On définit par récurrence la suite des entiers r_0,r_1,...,r_n tels que :*

- *r_0 est le reste de la division euclidienne de a par b.*
- *si $r_0 \neq 0$, r_1 est le reste de la division euclidienne de b par r_0.*
- *pour tout $k \in \{1; \ldots; n-1\}$, si $r_k \neq 0$, alors r_{k+1} est le reste de la division euclidienne de r_{k-1} par r_k.*

Alors cette suite d'entiers est nulle à partir d'un certain rang et la dernière valeur non nulle prise par cette suite est le pgcd d a et b.

Exercice 1. Appliquer l'algorithme d'Euclide pour déterminer le *pgcd* de 450 et 198.

1. Créer une fonction récursive pgcd qui prend en paramètres d'entrée deux entiers a et b puis calcule leur pgcd.
2. On note P_n la probabilité que deux entiers a,b tirés au hasard entre 1 et n soient premiers entre eux.
   - Écrire une fonction qui approxime P_n.
   - Lorsque n devient grand, comparer P_n et $\frac{6}{\pi^2}$

Euclide étendu

Théorème 1 (Théorème de Bézout)**.** *Deux entiers relatifs a et b sont premiers entre eux si et seulement s'il existe u et v tels que $au + bv = 1$.*

Remarque : Il n'y a pas unicité des entiers u et v tels que $au + bv = 1$.

Exercice 2. Déterminer deux entiers u et v tels que $29u + 12v = 1$.

1. Justifier qu'il existe bien un couple d'entiers $(u; v)$ tel que $29u + 12v = 1$.
2. Appliguer l'algorithme d'Euclide pour connaître les restes successifs jusqu'au reste égal à 1.
3. Utiliser les divisions euclidiennes obtenues en remontant l'algorithme pour déterminer u et v.

Exercice 3. Justifier l'existence d'un couple d'entiers $(u; v)$ tels que $130u + 231v = 1$ et en déterminer un.

Pour obtenir ces coefficients de Bézout, on peut donc utiliser l'algorithme d'Euclide qui permet de calculer le $Pgcd(a,b)$ d de a et de b. Pour cela, on exprime, à chaque étape de l'algorithme, le reste obtenu en fonction de a et de b par une expression de la forme :

$$au_n + bv_n = r_n.$$

À la fin de l'algorithme, le dernier reste non nul est le $Pgcd(a,b)$ d de a et de b, la relation ci-dessus donne donc les coefficients de Bézout recherchés.

Écrivons la relation à deux rangs consécutifs $n-1$ et n :

$$\begin{cases} au_{n-1} + bv_{n-1} = r_{n-1} \\ au_n + bv_n = r_n \end{cases}$$

L'étape suivante dans l'algorithme d'Euclide, si $r_n \neq 0$, consiste à effectuer la division euclidienne de r_{n-1} et de $r_{n-1} = qr_n + r_{n+1}$: $r_{n-1} = qr_n + r_{n+1}$ avec $0 \leqslant r_{n+1} < r_n$.

On a donc :

$$\begin{aligned} r_{n+1} &= r_{n-1} - qr_n \\ &= au_{n-1} + bv_{n-1} - q(au_n + bv_n) \\ &= a(u_{n-1} - qu_n) + b(v_{n-1} - qv_n) \end{aligned}$$

On pose donc :

$$\begin{cases} u_{n+1} = u_{n-1} - qu_n \\ v_{n+1} = v_{n-1} - qv_n \end{cases} \quad (2)$$

Il s'agit d'une récurrence double, qu'on initialise en posant :

$$\begin{cases} u_0 = 1 \text{ et } v_0 = 0 & \text{car } 1 \times a + 0 \times b = a \\ u_1 = 0 \text{ et } v_1 = 1 & \text{car } 0 \times a + 1 \times b = b \end{cases}$$

1. Construire les suites (u_n) et (v_n) déterminant les coefficients de Bézout pour $a = 47$ et $b = 35$.
2. Écrire une fonction `euclide_etendu` qui prend en paramètres a et b puis renvoie le *pgcd*, puis les coefficients u,v tels que $au + bv = pgcd(a,b)$