CC1 : Algorithme d'Euclide

Durée de l'épreuve : 1h30

Vous pouvez répondre aux questions de manière concise, mais la précision de vos réponses sera un élément important de la notation des copies. À elles seules, les parties I et II peuvent donner une note fort respectable (17/20 si les réponses sont correctes et brièvement justifiées) et la partie III permettra de gagner des points supplémentaires (et/ou de compenser d'éventuelles erreurs dans les parties précédentes).

I. Rappels

Soient a et b deux éléments de $\mathbb{Z}$.

Si $b \neq 0$, l'instruction python "`a//b`" calcule le quotient de la division euclidienne de a par b. De plus, l'instruction "`a%b`" calcule le reste de cette division euclidienne.

De plus, si $a < b$, `range(a,b)` calcule la liste `[a,a+1,a+2,...,b-1]` (liste qui compte b-a éléments). En revanche si $a \geqslant b$, alors `range(a,b)` est la liste vide (c'est à dire `[]`).

On rappelle aussi que la notation $a|b$ signifie "a est un diviseur de b" et est définie par : $a|b \Leftrightarrow \exists k \in \mathbb{Z} : b = a \cdot k$

Enfin, si $a \neq 0$ ou $b \neq 0$, le PGCD de a et b, noté $PGCD(a,b)$ est le plus grand diviseur commun de a et b, c'est à dire :

$$PGCD(a,b) = max(\{d \in \mathbb{Z} \text{ tel que } d|a \text{ et } d|b\}) \tag{1}$$

Pour chaque question de cette partie, on vous demande une démonstration de votre réponse, s'appuyant sur cette définition du PGCD.

I.1 Premières propriétés du PGCD :

1. Soit $n \in \mathbb{N}^*$. Que vaut $PGCD(n,0)$?
2. Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.
   (a) Montrer que $PGCD(a,b)$ est bien défini, au sens où l'ensemble des diviseurs commun a bien un maximum.
   (b) Les nombres $PGCD(a,b)$ et $PGCD(|a|,|b|)$ sont-ils nécessairement égaux ?
   (c) Soit $k \in \mathbb{Z}$. Les nombres $PGCD(a,b)$ et $PGCD(a + b\,k,b)$ sont-ils nécessairement égaux ?

I.2 Algorithme d'Euclide

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$.

On définit les suites a_n et b_n par récurrence par :

- $a_0 = a$ et $b_0 = b$
- pour $n \in \mathbb{N}$ tel que $b_n \neq 0$, on pose $a_{n+1} = b_n$ et $b_{n+1} = R$ où R désigne le reste de la division euclidienne de a_n par b_n.
- pour $n \in \mathbb{N}$ tel que $b_n = 0$, on pose $a_{n+1} = a_n$ et $b_{n+1} = b_n$

1. Montrer que $\forall n \in \mathbb{N}$, $PGCD(a_n,b_n) = PGCD(a,b)$.

2. Montrer que la suite b_n est décroissante. Est-elle strictement décroissante ? Montrez qu'elle est nulle à partir d'un certain rang, en déduire que a_n a une limite et identifier cette limite.

II Calcul du pgcd

Trois étudiants écrivent chacun une fonction `pgcd` en Python qui calcule le pgcd de deux entiers a et b (en supposant que a et b ne sont pas tous les deux nuls).

Pour chacune de leurs réponses (proposées ci-dessous) :

- Déterminer ce que renvoie Python quand on exécute `pgcd(0,2)`, `pgcd(2,2)` et `pgcd(4,2)`
- Justifier si la fonction proposée par l'étudiant est correcte.
- Si la réponse proposée par l'étudiant n'est pas correcte, proposez une modification qui la rend correcte.

II.1 Réponse du premier étudiant

```
def pgcd(a,b):
    if b==0: return a
    Q,R=(a//b,a%b)
    return pgcd(R,b)
```

II.2 Réponse du deuxième étudiant

```
def pgcd(a,b):
    m=min(abs(a),abs(b))
    M=max(abs(a),abs(b))
    if m==0:
        return M
    return pgcd(M-m,m)
```

II.3 Réponse du troisième étudiant

```
def pgcd(a,b):
    R=0
    for d in range(1,min(abs(a),abs(b))+1):
        if a%d==0 and b%d==0:
            R=d
    return R
```

III Question d'arithmétique

On rappelle que le PPCM de deux entiers satisfait la relation $PGCD(a,b) \times PPCM(a,b) = a \times b$.

Écrire un programme qui, quand on lui donne deux nombre g et p, trouve tous les $(a,b) \in \mathbb{N}^2$ tels que $PGCD(a,b) = g$ et $PPCM(a,b) = p$.