

TD 1

DIVISIBILITÉ, PGCD ET ALGORITHMES D'EUCLIDE

Exercice 1. Pour tout $a, b, c \in \mathbb{Z}$, montrer que :

- 1) $a \mid b$ et $a \mid c \Rightarrow a \mid (b + c)$ and $a \mid (b - c)$.
- 2) $a \mid b$ et $b \mid c \Rightarrow a \mid c$.
- 3) $a \mid b$ et $b \mid a \Rightarrow a = \pm b$.
- 4) $a \mid 1 \Leftrightarrow a = \pm 1$.

Exercice 2. En cours, nous avons vu la version originale de l'algorithme d'Euclide :

Algorithme 1 : Algorithme d'Euclide (version originale)

Entrées : Deux entiers $a, b > 0$

Sorties : Le pgcd de a et b

```

1 fonction EuclideSoustractif( $a, b$ ) :
2   tant que  $a \neq b$  faire
3     si  $a > b$  alors
4        $a \leftarrow a - b$ 
5     sinon
6        $b \leftarrow b - a$ 
7   retourner  $a$ 

```

Montrer que l'algorithme est correct, c'est-à-dire :

- 1) montrer que l'algorithme termine.
- 2) montrer que l'algorithme renvoie effectivement $\text{pgcd}(a, b)$. Pour cela, il suffit de prouver que si $a > b$ alors :

$$\text{pgcd}(a, b) = \text{pgcd}(a - b, b).$$

- 3) Quelle est la complexité de l'algorithme dans le pire des cas ?

Exercice 3. Soient a, b, c des entiers non nuls avec $c > 0$. Montrer que :

- 1) $\text{pgcd}(ac, bc) = c \text{pgcd}(a, b)$;
- 2) si $\text{pgcd}(a, b) = d$ alors les entiers $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.

Exercice 4. En appliquant l'algorithme d'Euclide étendu, calculer le pgcd et le couple (u, v) de l'identité de Bézout pour les couples de nombres suivants :

- 1) 13 et 21 ;

2) 2926 et 2046.

Exercice 5 On rappelle que la suite de Fibonacci $(F(n))_{n \geq 0}$ est définie par $F(0) = 0$, $F(1) = 1$ et $F(n) = F(n-1) + F(n-2)$ pour $n \geq 2$. Le but de cet exercice est d'étudier le comportement de l'algorithme d'Euclide classique sur des entiers de Fibonacci consécutifs.

- 1) Appliquer une étape de l'algorithme d'Euclide classique (division euclidienne) au couple $(F(n+1), F(n))$, pour $n \geq 2$. Que remarque-t-on sur le reste obtenu ?
- 2) En déduire le nombre d'étapes effectuées par l'algorithme sur ce couple avant d'atteindre un reste nul.
- 3) Pourquoi les nombres de Fibonacci consécutifs constituent-ils un cas particulièrement défavorable pour l'algorithme d'Euclide ?

Cela montre que les couples d'entiers de Fibonacci consécutifs réalisent le pire cas de l'algorithme d'Euclide classique : à taille (nombre de chiffres) fixée, aucun couple d'entiers ne nécessite plus d'étapes. Comme $F(n)$ croît exponentiellement vite en n (donc le nombre de chiffres de $F(n)$ est de l'ordre de n), on en déduit que le nombre d'étapes de l'algorithme d'Euclide classique est toujours $O(n)$, où n est le nombre de chiffres des entrées.

Exercice 6. Soient $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$, et soit $d = \text{pgcd}(a, b)$.

- 1) Montrer que s'il existe $s, t \in \mathbb{Z}$ tels que $as + bt = r$, alors $d \mid r$.
- 2) Montrer que si (u, v) forment une paire d'entiers satisfaisant l'identité de Bézout $d = au + bv$, alors $\text{pgcd}(u, v) = 1$.

Exercice 7. Soient $a, b_1, \dots, b_k \in \mathbb{Z}$. Montrer que $\text{pgcd}(a, b_1 b_2 \cdots b_k) = 1$ si et seulement si $\text{pgcd}(a, b_i) = 1$ pour tout $i = 1, \dots, k$.

Exercice 8. Soit a et b deux entiers et d leur pgcd. Par simplicité, on suppose a et b strictement positifs.

1. Montrer qu'il existe une infinité de couples de coefficients de Bézout (u, v) tels que $au + bv = d$.
[Indice : Ajouter et retrancher ab au membre de gauche de l'équation.]
2. Soit (u, v) des coefficients de Bézout associés à a et b . Montrer qu'un couple (u', v') satisfait $au' + bv' = d$ si et seulement s'il existe k tel que $u' = u + k \frac{b}{d}$ et $v' = v - k \frac{a}{d}$.
3. Montrer qu'il existe exactement deux couples de coefficients de Bézout tels que $|u| \leq \frac{b}{d}$ et $|v| \leq \frac{a}{d}$.