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

```
fonction EuclideSoustractif(a, b) :
    tant que a ≠ b faire
        si a > b alors
            a ← a − b
        sinon
            b ← b − a
    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 $\mathrm{pgcd}(a, b)$. Pour cela, il suffit de prouver que si $a > b$ alors :

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

Exercice 3. 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 4. Soient a, b, c des entiers non nuls avec $c > 0$. Montrer que :

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

Exercice 5. Soient $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$, et soit $d = \mathrm{pgcd}(a, b)$.

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 $\mathrm{pgcd}(u, v) = 1$.

Exercice 6. Soient $a, b_1, \ldots, b_k \in \mathbb{Z}$. Montrer que $\mathrm{pgcd}(a, b_1 b_2 \cdots b_k) = 1$ si et seulement si $\mathrm{pgcd}(a, b_i) = 1$ pour tout $i = 1, \ldots k$.

Exercice 7. 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 $|v| \leq \frac{a}{d}$.