Plus grand commun diviseur Soit a et b deux entiers **relatifs**.

Définition : $c \in \mathbb{Z}$ est un diviseur commun à a et à b si $c|a$ et $c|b$

Définition Le plus grand commun diviseur à a et à b est **le plus grand** élément des diviseurs communs **positifs** de a et b

Exercice 1 Montrer que cette définition a un sens

Notation On note pgcd(a,b) le plus grand commun diviseur de a et de b

Exemple : pgcd(-30,21) = pgcd(30,21) = 3

Exercice 2

Prouver

1. pgcd(a,b) = pgcd($|a|$,$|b|$)
2. pgcd(a,ka) = $|a|$ pour tout $k \in \mathbb{Z}$
3. pgcd(a,b) = pgcd($a - b$,b)
4. pgcd(ka,kb) = |k|pgcd(a,b) pour tout $k \in \mathbb{Z}$
5. pgcd(a,b) = pgcd(b,r) où $b > 0$ et $a = bq + r$ avec $0 \leqslant r < b$

Exercice 3

En utilisant 1) et 5) ci-dessus on peut écrire

$a = bq_1 + r_1$ avec $0 \leqslant r_1 < b$

$b = r_1q_2 + r_2$ avec $0 \leqslant r_2 < r_1$

$r_1 = r_2q_3 + r_3$ avec $0 \leqslant r_3 < r_2$

plus généralement

$r_{n-2} = r_{n-1}q_n + r_n$ avec $0 \leqslant r_n < r_{n-1}$

$r_{n-1} = r_nq_{n+1} + r_{n+1}$ avec $0 \leqslant r_{n+1} < r_n$

1. Peut on avoir une suite **strictement décroissante** d'entiers naturels **non nuls** ? Justifier qu'il existe alors un entier naturel s tel que $r_{s-1} = r_sq_{s+1}$
2. En utilisant les propriétés vues dans l'exercice 3 montrer que pgcd(a,b) = r_s, le dernier reste non nul

Exercice 4

Soit a et b deux entiers **naturels** , on note $a\mathbb{Z}$+$b\mathbb{Z}$, l'ensemble des combinaisons linéaires de a et b

Prouver :

1. pgcd(a,b) divise tout élément de $a\mathbb{Z} + b\mathbb{Z}$
2. $a\mathbb{Z} + b\mathbb{Z}$ = pgcd(a,b)$\mathbb{Z}$

Autrement dit

Théorème de Bézout Pour tout a et b deux entiers naturels on peut exprimer le plus grand commun diviseur de a et de b comme une **combinaison linéaire** de a et b

Est ce que cette combinaison linéaire est **unique** ?

Définition Deux entiers relatifs sont **premiers entre eux** si leur pgcd vaut 1

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

Exercice 5

Comment trouver cette combinaison linéaire ? Réécrire $(r_{n-1}, r_n) -> (r_n, r_{n+1})$

Puisque nous savons que pgcd(a,b) est le dernier reste non nul des divisions successives dans l'algorithme d'Euclide, pour trouver cette combinaison linéaire on procède ainsi :

En posant $r_{-1} = a$ et $r_0 = b < a$ avec $r_{n-2} = r_{n-1}q_n + r_n$ on peut calculer les termes de la suite (r_n). Nous avons ici une récurrence double, pour déterminer r_n nous avons besoin des deux termes précédents et l'initialisation se fait avec les deux termes initiaux $r_{-1} = a$ et $r_0 = b < a$

1. Donner un algorithme qui met à jour le couple (r_{n-1}, r_n), un tour de boucle fait passer de (r_{n-1}, r_n) à (r_n, r_{n+1})
2. On veut qu'un invariant de boucle est que chaque reste r_k soit une combinaison linéaire de a et b.
   En partant de $r_{-1} = a = 1 \times a + 0 \times b = u_{-1}a + v_{-1}b$ et $r_0 = b = 0 \times a + 1 \times b = u_0a + v_0b$, on veut construire par récurrence deux suites (u_n) et (v_n) telles que : $r_n = u_na + v_nb$ et $u_{-1} = 1$, $u_0 = 0$ et $v_{-1} = 0$, $v_0 = 1$, il nous reste à trouver une relation de récurrence reliant $w_n = (u_n, v_n)$ à $w_{n-1} = (u_{n-1}, v_{n-1})$ et $w_{n-2} = (u_{n-2}, v_{n-2})$
   Vérifier que cette relation est $w_n = w_{n-2} - \lfloor \frac{r_{n-2}}{r_{n-1}} \rfloor w_{n-1}$
3. Donner l'algorithme d'Euclide étendu où un tour de boucle met à jour deux couples de variables $(r_{n-1}, r_n) -> (r_n, r_{n+1})$ et $(w_{n-1}, w_n) -> (w_n, w_{n+1})$

Exercice 7

Décomposition en nombres premiers et pgcd de deux entiers

Prouver que si on peut décomposer deux entiers a et b en facteurs premiers alors le pgcd de a et b est obtenu en prenant les facteurs premiers communs avec les exposants au minimum des deux exposants

Exercice 6

Prouver le **Théorème de Gauss** si $a|bc$ et si a et b sont **premiers entre eux** alors $a|c$

Plus petit commun multiple Les multiples communs à a et à b sont les éléments de $a\mathbb{Z} \cap b\mathbb{Z}$.

Ce sont les multiples du plus petit commun multiple de a et b noté ppcm(a,b)

Exercice 8 Décomposition en nombres premiers et ppcm de deux entiers

Prouver que si on peut décomposer deux entiers a et b en facteurs premiers alors le ppcm de a et b est obtenu en prenant tous les facteurs premiers et lorsqu'il y a des facteurs communs on les prend avec les exposants au maximum des deux exposants