Algorithme d'Euclide étendu, Théorème de Bézout

1. Anneaux

Soit A un anneau et soit E un ensemble non-vide. On note $\mathcal{F}(E, A)$ l'ensemble des fonctions de E dans A.

Si $f, g \in \mathcal{F}(E, A)$, on définit la somme $f+g$ et le produit $f \cdot g$ par les équations

$$\begin{aligned} (f+g)(x) &= f(x)+g(x), \quad \text{pour tout } x \in E \\ (f \cdot g)(x) &= f(x) \cdot g(x), \quad \text{pour tout } x \in E \end{aligned}$$

- Montrer que l'ensemble $\mathcal{F}(E, A)$ muni des deux lois binaires

$(f, g) \mapsto f+g \quad \text{et} \quad (f, g) \mapsto f \cdot g,$ est un anneau.

- Montrer que cet anneau est commutatif si A est un anneau commutatif. Quels sont les éléments neutres de cette anneau pour l'addition et la multiplication?

2. Algorithme d'Euclide

1. Montrer que si a et b sont deux entiers tels que $a > b$, alors $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, a \mod b)$.
2. Calculer le pgcd de $a = 105$ et $b = 12$.

3. Algorithme d'Euclide étendu

Soient $a = 167$ et $b = 115$.

1. Calculer le $\operatorname{pgcd}(a, b)$ en utilisant l'algorithme d'Euclide.
2. Calculer $u, v \in \mathbb{Z}$ tels que $a \cdot u + b \cdot v = \operatorname{pgcd}(a, b)$.
3. Calculer l'inverse de b modulo a.

Faire le même exercice avec $a = 153$ et $b = 140$.

4. Éléments inversibles

1. Énumérer tous les éléments inversibles de $\mathbb{Z}/16\mathbb{Z}$.
2. Énumérer tous les éléments inversibles de $\mathbb{Z}/11\mathbb{Z}$.
3. Montrer que si a et b sont deux éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$, alors l'élément ab est également inversible.
4. Montrer que l'ensemble $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour la multiplication.

5. Petit théorème de Fermat

Le petit théorème de Fermat s'annonce comme suit: Si p est un nombre premier et a un entier qui n'est pas divisible par p, alors

$$a^{p-1} \equiv 1 \mod p.$$

On utilisera ce résultat sans preuve.

1. Calculer l'aide du petit théorème de Fermat :

- $2^{751} \mod 31$
- $2^{32410} \mod 53$