Master CSI 1

Arithmétique 1

Feuille d'exercices n° 1.

L'algorithme d'Euclide, d'Euclide étendu, Bezout, et application à l'inversion modulaire

1 Trouvez le pgcd et une relation de Bezout pour les couples (a, b) suivants :

$$(34, 21), \quad (136, 51), \quad (481, 325)$$

puis répondez aux questions :
- a est-il inversible modulo b ? Si oui quel est son inverse ?
- b est-il inversible modulo a ? Si oui quel est son inverse ?

2 Trouvez le pgcd et une relation de Bezout pour les couples (f, g) d'éléments de $\mathbb{Z}/p\mathbb{Z}[X]$ suivants :

1. $f = X^3 + X + 1$, $g = X^2 + X + 1$, $p = 2$, puis $p = 3$
2. $f = X^4 + X^3 + X + 1$, $g = X^3 + X^2 + X + 1$, $p = 2$, puis $p = 3$
3. $f = X^5 + X^4 + X^3 - X^2 - X + 1$, $g = X^3 + X^2 + X + 1$, $p = 3$, puis $p = 5$

3 Soit $f = X^4 + X^3 + 2X^2 + X + 1$, $g_1 = X$, $g_2 = X^3 + X$ dans $\mathbb{Q}[X]$. Calculez des polynômes t_1, t_2 tels que $t_i g_i \equiv 1 \mod f$ s'ils existent. Le quotient $\mathbb{Q}[X]/f(X)\mathbb{Q}[X]$ est-il un corps ?

4 Soit $g = X^5 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$. Pour les polynômes :

1. $f = X^3 + X + 1$
2. $f = X^3 + 1$

si f est inversible modulo g trouvez son inverse ; si f n'est pas inversible modulo g expliquez pourquoi f est un diviseur de zéro modulo g (c'est-à-dire un diviseur de zéro de l'anneau quotient $\mathbb{Z}/2\mathbb{Z}[X]/f(X)\mathbb{Z}/2\mathbb{Z}[X]$) et trouvez un polynôme h de degré inférieur à 5 tel que $fh \equiv 0 \mod g$.

5 Trouvez un polynôme $f \in \mathbb{Z}/7\mathbb{Z}[X]$ de degré inférieur à 4 et vérifiant :

$$(X^2 - 1)f \equiv X^3 + 2X + 5 \mod X^4 + 2X^2 + 1$$