

TD 1 – Entiers et entiers modulaires

Exercice 1.

Euclide

1. À l'aide de l'algorithme d'Euclide (version itérative), calculer le PGCD des couples
 - i. (27, 31) ;
 - ii. (21, 15).
2. À l'aide de l'algorithme d'Euclide étendu, calculer le PGCD et les coefficients de Bézout du couple (22, 14).
3. Soit a et b deux entiers et d leur PGCD. *Par simplicité, on suppose a et b strictement positifs.*
 - i. Montrer qu'il existe une infinité de couples de coefficients de Bézout (u, v) tels que $au + bv = d$. *Ajouter et retrancher ab à l'égalité, et réorganiser.*
 - ii. 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 $u' = u + k\frac{b}{a}$ et $v' = v - k\frac{a}{a}$.
 - iii. Montrer qu'il existe exactement deux couples de coefficients de Bézout tels que $|u| \leq \frac{b}{a}$ et $|v| \leq \frac{a}{a}$.

Exercice 2.

Factorisation et PGCD

1. Montrer qu'il existe une infinité de nombres premiers. *Supposer à l'inverse que seuls p_1, \dots, p_k sont premiers, et considérer $p_1 \cdots p_k + 1$.*
2.
 - i. Soit n, e, f des entiers positifs. Montrer que n^e divise n^f si et seulement si $f \geq e$.
 - ii. Soit $a = \prod_{i=1}^k p_i^{e_i}$ la décomposition en facteurs premiers de a . Montrer qu'un entier b divise a si et seulement s'il existe f_1, \dots, f_k tels que $b = \prod_{i=1}^k p_i^{f_i}$ et $0 \leq f_i \leq e_i$.
 - iii. Avec les mêmes notations, montrer que $\text{PGCD}(a, b) = \prod_{i=1}^k p_i^{\min(e_i, f_i)}$.

Exercice 3.

Entiers modulaires

1. Écrire les tables d'addition et de multiplication de $\mathbb{Z}/6\mathbb{Z}$.
2. Lister l'ensemble $(\mathbb{Z}/14\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/14\mathbb{Z}$.
3. Résoudre les équations $21z \equiv_{30} 12$ et $14z \equiv_{21} 5$.
4. Résoudre dans \mathbb{Z} les systèmes suivants :

$$\begin{cases} z \equiv_7 1 \\ z \equiv_5 3 \end{cases}, \quad \begin{cases} z \equiv_2 0 \\ z \equiv_3 1 \\ z \equiv_5 0 \end{cases}.$$

Exercice 4.*Racines carrées de 1*

1. Montrer que $[1]$ et $[n-1]$ sont des racines carrées de $[1]$ dans $\mathbb{Z}/n\mathbb{Z}$.
2. Trouver d'autres racines carrées de $[1]$ dans $\mathbb{Z}/15\mathbb{Z}$.
3. Existe-t-il d'autres racines carrées de $[1]$ dans $\mathbb{Z}/7\mathbb{Z}$?
4. Soit p un nombre premier et α une racine carrée de $[1]$ dans $\mathbb{Z}/p\mathbb{Z}$.
 - i. Soit a le représentant canonique de α . Montrer que $(a-1)(a+1)$ est un multiple de p .
 - ii. En déduire que $a = 1$ ou $p-1$.
 - iii. Conclure.

Exercice 5.*Équations du second degré*

On dit qu'un élément $\alpha \in \mathbb{Z}/n\mathbb{Z}$ est un carré s'il existe $\beta \in \mathbb{Z}/n\mathbb{Z}$ tel que $\alpha = \beta \times \beta$.

1. Lister les carrés de $\mathbb{Z}/13\mathbb{Z}$.

Soit p un nombre premier différent de 2.

2. On veut montrer qu'une équation du second degré $\chi^2 + \alpha\chi + \beta = 0$ admet une solution dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si son discriminant $\alpha^2 - 4\beta$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
 - i. Montrer que les puissances de 2 sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$.
 - ii. On suppose que l'équation admet une solution χ . Montrer que $(\chi + [2]^{-1}\alpha)^2 = [4]^{-1}\alpha^2 - \beta$. En déduire que le discriminant est un carré.
 - iii. Réciproquement, montrer que si $\alpha^2 - 4\beta = \delta^2$, alors $\chi = [2]^{-1}(\delta - \alpha)$ est solution de l'équation.
3. Résoudre les équations $\chi^2 + 3\chi + 5 = 0$ et $\chi^2 + 4\chi + 8 = 0$ dans $\mathbb{Z}/13\mathbb{Z}$.
Donner toutes les solutions.