CC1 du 8/10/2024 - Algèbre M1 MIC (MA6AY040)

15h15-16h45 (1h30)
Sans documents ni calculatrices.

Exercise 1

1. ($\simeq$ 6 points) On rappelle que $901 = 53 \cdot 17$.
   (a) Donnez (sous forme factorisée) le cardinal du groupe multiplicatif $(\mathbb{Z}/901\mathbb{Z}, \cdot\,)^\times$.

> **Solution:** Le cardinal du groupe des unités est donné par l'indicatrice d'Euler, qui est multiplicative (pour les nombres premiers entre eux), donc :
>
> $$\varphi(901) = \varphi(53 \cdot 17) = \varphi(53\dot{1}7).$$
>
> Les deux nombres 53 et 17 sont premiers, et si p est premier, on a que $\varphi(p) = p - 1$. On en déduit que :
>
> $$\varphi(901) = (53-1)(17-1) = 52 \cdot 16 = 832 = 2^6 \cdot 13.$$

   (b) Existe-t-il un élément d'ordre 32 dans $(\mathbb{Z}/901\mathbb{Z}, \cdot\,)^\times$? (justifier)

> **Solution:** D'après le théorème des restes chinois, et le fait que le groupe des unités de $\mathbb{Z}/p\mathbb{Z}$ est cyclique quand p est premier, on a :
>
> $$(\mathbb{Z}/901\mathbb{Z})^\times \cong (\mathbb{Z}/53\mathbb{Z})^\times \times (\mathbb{Z}/17\mathbb{Z})^\times \cong \mathbb{Z}/52\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}.$$
>
> Les ordres des éléments de $\mathbb{Z}/52\mathbb{Z}$ divisent 52, tandis que ceux que $\mathbb{Z}/16\mathbb{Z}$ divisent 16. Les ordres des éléments du produit divisent donc le PPCM $52 \vee 16 = 208$. Or, 32 ne divise pas 208, donc le groupe ne contient pas d'élément d'ordre 32.

   (c) Déterminer si 901 est un carré modulo 41.

> **Solution:** On cherche à calculer le symbole de Legendre $\left(\frac{901}{41}\right)$. Or, $901 = 22 \cdot 41 - 1 \equiv -1 \pmod{41}$, donc d'après le premier complément de la loi de réciprocité quadratique :
>
> $$\left(\frac{901}{41}\right) = \left(\frac{-1}{41}\right) = (-1)^{\frac{41-1}{2}} = 1.$$

   (d) Déterminer si 41 est un carré modulo 901 et calculer le symbole de jacobi $\left(\frac{41}{901}\right)$.

> **Solution:** Pour que 41 soit un carré modulo $901 = 17 \cdot 53$, il faut et il suffit qu'il soit un carré modulo 17 et un carré modulo 53. En appliquant plusieurs fois la loi de réciprocité quadratique et la multiplicativité du symbole de Jacobi, on trouve que :
>
> $$\left(\frac{41}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1;$$
>
> $$\left(\frac{41}{53}\right) = \left(\frac{53}{41}\right) = \left(\frac{12}{41}\right) = \left(\frac{3}{41}\right)\left(\frac{2}{41}\right)^2 = \left(\frac{3}{41}\right) = \left(\frac{41}{3}\right) = \left(\frac{2}{3}\right) = -1.$$
>
> Donc 41 n'est ni un carré mod 17 ni mod 53, donc ce n'est pas un carré mod 901. Cependant, par multiplicativité, on trouve que $\left(\frac{41}{901}\right) = 1$.

2. ($\simeq$ 3 points) Effectuez l'algorithme d'Euclide étendu pour le couple $(909, 53)$ en détaillant les résultats à chaque itération, et donnez une solution entière à l'équation :

$$909u + 53v = 1$$

Solution:

```
 2, [909,1,0]
17, [53,0,1]
 6, [8,1,-17]
 1, [5,-6,103]
 1, [3,7,-120]
 1, [2,-13,223]
    [1,20,-343]
```

3. ($\simeq$ 3 points) Résoudre dans $\mathbb{Z}$ le système suivant :

$$\begin{cases} 2x & \equiv -1 \pmod{101} \\ x & \equiv -3 \pmod{9} \\ x & \equiv 20 \pmod{53} \end{cases}$$

Solution: Notons déjà que $2x \equiv -1 \pmod{101}$ admet $x = 50$ comme solution assez évidente. Commençons par résoudre les deux premières équations. Si $x \equiv 50 \pmod{101}$, alors on écrit $x = 50 + 101k$; on remplace dans la deuxième équation pour avoir :

$$50 + 101k \equiv -3 \pmod{9} \iff 5 + 2k \equiv -3 \pmod{9} \iff 2k \equiv 1 \pmod{9}.$$

On en déduit que $k \equiv 5 \pmod{9}$, c'est-à-dire que :

$$\begin{cases} 2x & \equiv -1 \pmod{101} \\ x & \equiv -3 \pmod{9} \end{cases} \iff x \equiv 555 \pmod{909}.$$

On cherche donc à résoudre le système :

$$\begin{cases} x & \equiv 555 \pmod{909} \\ x & \equiv 20 \pmod{53}. \end{cases}$$

Posons $x = 555 + 909l$ avec $l \in \mathbb{Z}$. On substitue dans la deuxième équation et on utilise la question précédente pour avoir que $909 \cdot 20 \equiv 1 \pmod{53}$:

$$909l \equiv -5 \pmod{53} \iff l \equiv -100 \pmod{53} \iff l \equiv 6 \pmod{53}.$$

On trouve donc :

$$x = 555 + 909 \cdot 6 + 53 \cdot 909l' = 6009 + 48177l' \equiv 6009 \pmod{53 \cdot 909}.$$

Exercise 2

On considère un nombre premier p impair que l'on suppose être un diviseur de

$$3^{\frac{p-1}{2}} + 1.$$

1. ($\simeq$ 1 points) Montrer que $\left(\frac{3}{p}\right) = -1$.

Solution: D'après le critère d'Euler :

$$\left(\frac{3}{p}\right) \equiv 3^{\frac{p-1}{2}} \pmod{p}.$$

Or, par hypothèse, $3^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. On en déduit que $\left(\frac{3}{p}\right)$ est congru à -1 mod p ; or, $p \geq 2$ et $\left(\frac{3}{p}\right) = \pm 1$, donc $\left(\frac{3}{p}\right) = -1$.

2. ($\simeq$ 2 points) En déduire que $p \equiv \pm 5 \pmod{12}$.

Solution: Pour appliquer la loi de réciprocité quadratique, distinguons deux cas :
- Si $p \equiv 1 \pmod 4$, on a que $\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right) = -1$, donc $p \equiv 2 \pmod 3$. En résolvant le problème des restes chinois, on trouve que l'on doit avoir $p \equiv 5 \pmod{12}$.
- Sinon, si $p \equiv 3 \pmod 4$, on a que $\left(\frac{p}{3}\right) = -\left(\frac{3}{p}\right) = 1$. On en déduit que $p \equiv 1 \pmod 3$. En résolvant le problème des restes chinois, on en déduit que $p \equiv -5 \pmod{12}$.

Exercise 3

1. ($\simeq$ 1 points) L'anneau $\mathbb{Z}/41\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z}$ est-il un anneau intègre ?

Solution: Non : l'élément $(1, 0)$ est un diviseur de zéro.

2. ($\simeq$ 2.5 points) On considère les morphismes d'anneaux suivant :

$$f\colon \begin{array}{ccc} \mathbb{Z}/41\mathbb{Z}[X] & \longrightarrow & (\mathbb{Z}/41\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z}) \\ P & \longmapsto & (P(6), P(-6)) \end{array} \quad \text{et} \quad g\colon \begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & (\mathbb{Z}/41\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z}) \\ P & \longmapsto & (P(6), P(-6)) \end{array}$$

   (a) Quels sont les noyaux de f et de g ?

Solution: Le noyau de f est l'ensemble des polynômes divisibles par $X - 6$ et $X + 6$. C'est donc l'ensemble des polynômes divisibles par leur PPCM, à savoir $(X - 6)(X + 6) = X^2 - 36$, i.e.,

$$\ker(f) = (X^2 - 36).$$

Le noyau de g est $g^{-1}(\ker(f))$. Il est donc engendré par 41 et $X^2 - 6$, i.e.,

$$\ker(g) = (41, X^2 - 36).$$

   (b) Le noyau de g est-il un idéal principal de $\mathbb{Z}[X]$?

Solution: Supposons que $\ker(g) = (Q)$ avec $Q \in \mathbb{Z}[X]$. Alors Q divise 41, donc Q est une constante. De plus, Q divise $X^2 - 36$, donc il divise son coefficient dominant, donc Q divise 1. On en déduit que $Q = \pm 1$. C'est absurde, car $g(1) = (1, 1) \neq (0, 0)$. Donc $\ker(g)$ n'est pas principal.

3. ($\simeq$ 1.5 points) On considère un nombre premier p congru à 9 modulo 20. L'idéal

$$I = (p, X^2 + 5)$$

de $\mathbb{Z}[X]$ est-il premier ?

Solution: Non cet idéal n'est pas premier. En effet, le quotient est isomorphe à $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+5)$. Or, nous allons montrer que le polynôme $X^2 + 5$ admet des racines. En effet, il admet une racine, si et seulement si -5 serait un résidu quadratique mod p. Or,

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right).$$

Comme $p \equiv 9 \pmod{20}$, on a $p \equiv 1 \pmod 4$, donc $(-1)^{\frac{p-1}{2}} = 1$. De même, $p \equiv 4 \pmod 5$, qui est un carré, donc $\left(\frac{p}{5}\right) = 1$. On a donc $\left(\frac{-5}{p}\right) = 1$, i.e., -5 est un carré modulo p.