Licence 2- 2020/2021

HLMA304 : Arithmétique

Thierry mignon

Octobre 2020

Feuille de TD n°2

1 Relations d'équivalences

Exercice 1. Soit $\mathcal{P}^*$ l'ensemble des nombres premiers strictement supérieur à 2. On définit une relation R sur $\mathcal{P}^*$ par :

$$\forall (p,q) \in (\mathcal{P}^*)^2,\ \frac{p+q}{2} \in \mathcal{P}^*$$

Est-ce une relation d'équivalence ?

Exercice 2. ($\star$) Soit E un ensemble fini non vide, et x un élément de E. Les relations $\sim$ définie ci-dessous sont-elles des relations d'équivalences sur l'ensemble $\mathcal{P}(E)$ des parties de E ?

1. $\forall A, B \in \mathcal{P}(E), A \sim B \iff x \in A \cup B$

2. $\forall A, B \in \mathcal{P}(E), A \sim B \iff (x \in A \cup B \text{ ou } x \in \overline{A} \cap \overline{B})$

Exercice 3. ($\star$) On définit la relation $\sim$ sur $\mathbb{Z}$ par $x \sim y \iff x^2 \equiv y^2$ [5].

(1) Déterminer l'ensemble quotient, en donnant un représentant de chaque classe d'équivalence.

(2) L'addition de $\mathbb{Z}$ est-elle compatible avec cette relation ? et la multiplication ?

2 Relations de congruences

Exercice 4. Montrer que si a et b sont des entiers non multiples de 5, alors un, et un seul, des nombres a^2+b^2 et a^2-b^2 est multiple de 5.

Exercice 5. ($\star$) Montrer que parmi $n, n+2, n+4$ il y a au moins un nombre divisible par 3.

Exercice 6. Soit p un nombre premier. Montrer que $p+20$ et $p+22$ ne sont pas tous les deux des nombres premiers (restes modulo... ?).

Exercice 7. Montrer que les entiers congrus à -1 modulo 8 ne peuvent être somme de trois carrés.

Exercice 8. ($\star$) Chercher les restes modulo 9 possibles des cubes. Montrer que, si 9 divise $a^3+b^3+c^3$ alors 3 divise abc.

Exercice 9. Trouver les couples $(m,n) \in \mathbb{Z}^2$ tels que $n^6 - n^3 = 7m^2 + 3$ (restes modulo 7).

Exercice 10.

(1) Soit p un nombre premier. Soeint $m, n \in \mathbb{Z}$ tels que $m^2 \equiv n^2[p]$. Montrer que soit $m \equiv n[p]$, soit $m \equiv -n[p]$.

(2) Donner l'exemple de deux nombres entiers m et n tels que $m^2 \equiv n^2[8]$, mais $m \not\equiv \pm n[8]$.

(3) Montrer que $m^2 \equiv n^2[6]$ implique $m \equiv \pm n[6]$.

Exercice 11. Rappelons que $2^{10} = 1024$. Calculer le reste de la division de 2^{10^n} par 25.

Exercice 12. Quel est le dernier chiffre de 2^{123456} ? (Utiliser le fait que $2^4 \equiv 1[5]$).

Exercice 13. ($\star$) Quel est le dernier chiffre de $3^{123456789}$? (Indication : $3^2 \equiv -1[10]$ et $123456789 \equiv 1[4]$).

3 Groupes

Exercice 14. ($\star$) Soit $n \in \mathbb{N}^*$ et $G = \mathbb{Z}/n\mathbb{Z}$. Soit $k \in \mathbb{Z}$ et $d = \text{pgcd}(k,n)$.

(1) On appelle *ordre* de $\overline{k}$ le plus petit entier $a \in \mathbb{N}^*$ tel que $a.\overline{k} = \underbrace{\overline{k} + \cdots + \overline{k}}_{a \text{ termes}} = \overline{0}$.

Montrer que l'ordre de $\overline{k}$ dans G est n/d.

(2) Montrer que $\overline{k}$ et $\overline{d}$ engendrent le même sous-groupe de G.

Exercice 15. ($\star$) Soient a, b deux éléments d'un groupe multiplicatif G tels que :

$$\begin{cases} a \text{ est d'ordre } m \\ b \text{ est d'ordre } n \\ \text{pgcd}(m,n) = 1 \\ ab = ba. \end{cases}$$

Déterminer l'ordre de ab.

Exercice 16. ($\star$) *(Théorème de Lagrange)* Soit G un groupe fini et H un sous-groupe de G. On définit une relation sur G par :

$$\forall\ x, y \in G,\ x \sim y \iff \exists\ h \in H \text{ tq } x = hy.$$

(1) Montrer que $\sim$ est une relation d'équivalence. Quelle est la classe de e ?

(2) Soit $a \in G$. Montrer que l'application de H vers G qui envoie h sur ha réalise une bijection de H vers $\overline{a}$.

(3) En déduire que $\text{Card}\, H$ divise $\text{Card}\, G$.

4 Les anneaux $\mathbb{Z}/n\mathbb{Z}$

Exercice 17. Montrer que, si n est impair, alors la somme de tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ vaut $\overline{0}$.

Exercice 18. ($\star$) Montrer que les éléments inversibles de l'anneau $\mathbb{Z}/1024\mathbb{Z}$ sont exactement les classes impaires.

Exercice 19. Considérons la liste des anneaux suivants :

$$\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/11\mathbb{Z}, \mathbb{Z}/24\mathbb{Z}, \mathbb{Z}/25\mathbb{Z}, \mathbb{Z}/36\mathbb{Z}.$$

(1) Donner la liste de tous les éléments inversibles de chacun de ces anneaux.

(2) Pour chaque élément inversible de $\mathbb{Z}/10\mathbb{Z}$, trouver son inverse.

Exercice 20. Résoudre l'équation $x^2 = \overline{1}$ dans $\mathbb{Z}/5\mathbb{Z}$ (indication : écrire $(x - \overline{1})(x + \overline{1}) = \overline{0}$).

Exercice 21. On veut résoudre l'équation $x^2 = \overline{1}$ dans $\mathbb{Z}/10\mathbb{Z}$.

(1) En écrivant $(x-\overline{1})(x+\overline{1}) = \overline{0}$, utiliser les diviseurs de zéro de $\mathbb{Z}/10\mathbb{Z}$ pour montrer que, soit $(x - \overline{1}) \in \{\overline{0}, \overline{5}\}$, soit $(x + \overline{1}) \in \{\overline{0}, \overline{5}\}$.

(2) Tester les quatre valeurs possibles de x trouvées ci-dessus pour résoudre l'équation $x^2 = \overline{1}$ dans $\mathbb{Z}/10\mathbb{Z}$.

Exercice 22. ($\star$) Résoudre l'équation $x(x+\overline{1})$ dans $\mathbb{Z}/10\mathbb{Z}$.

Exercice 23. Montrer, en utilisant le petit théorème de Fermat que l'équation $x^2 = -\overline{1}$ n'a pas de solution dans $\mathbb{Z}/11\mathbb{Z}$.

Exercice 24. ($\star$) Soit p un nombre premier impair. Montrer que l'équation $x^2 = \overline{1}$ n'a pas de solution dans $\mathbb{Z}/2p\mathbb{Z}$ autre que $\overline{1}$ et $\overline{-1}$.

Exercice 25. Soient $p, q \in \mathbb{N} \setminus \{0,1,2\}$ tels que $\text{pgcd}(p,q) = 1$. Montrer que $x^2 = \overline{1}$ a bien une solution dans $\mathbb{Z}/pq\mathbb{Z}$ autre que $\overline{1}$ et $-\overline{1}$ (utiliser le lemme chinois).

Exercice 26. ($\star\star$) Trouver le cinquième chiffre en partant de la fin du nombre :

$$5^{5^{5^5}}$$

Exercice 27. ($\star\star$) Montrer que l'équation $y^2 = x^5 - 4$ n'a pas de solution entière.

5 Lemme chinois des restes

Exercice 28. Trouver toutes les solutions des systèmes suivants :

$$\begin{cases} x & \equiv 1[3] \\ x & \equiv 3[5] \\ x & \equiv 4[7] \\ x & \equiv 2[11] \end{cases} \quad , \quad \begin{cases} x & \equiv 997[2001] \\ x & \equiv 998[2002] \\ x & \equiv 999[2003] \end{cases}$$

Exercice 29.

(1) Quels sont les restes des division de 10^{100} par 13 et par 19 ?

(2) Quel est le reste de la division de 10^{100} par $247 = 13 \times 19$? En déduire que $10^{99}+1$ est multiple de 247.

Exercice 30. Déterminer la plus petite solution positive du système :

$$\begin{cases} x & \equiv 9[14] \\ x & \equiv 13[31] \end{cases}$$

Exercice 31. ($\star$) *(Fonction indicatrice d'Euler)* Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'éléments inversibles dans $(\mathbb{Z}/n\mathbb{Z}, \times)$.

(1) Calculer $\varphi(p)$ et $\varphi(p^\alpha)$ pour p premier et $\alpha \in \mathbb{N}^*$.

(2) Soient m et n premiers entre eux. On considère l'application $f : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ définie par $f(\overline{x}) = (\hat{x}, \tilde{x})$. Montrer que f est bien définie et réalise un isomorphisme d'anneaux.

(3) En déduire que $\varphi(mn) = \varphi(m)\varphi(n)$.

(4) Exprimer $\varphi(n)$ selon la décomposition primaire de n.