3MA262
Licence de mathématiques
Année académique 2023-2024

SCIENCES SORBONNE UNIVERSITÉ

Feuille d'exercices n° 2

Énoncés

Exercice 1 – Étant donnés deux entiers $a > 1$ et $n > 0$, montrer que n divise $\varphi(a^n - 1)$ et que $2n$ divise $\varphi(a^n + 1)$.

Exercice 2 – Montrer que pour tout entier n, l'entier $n^3(n^6 - 1)$ est divisible par 504.

Exercice 3– Étant donné un entier naturel n, l'entier $M_n = 2^n - 1$ est le ***n-ème nombre de Mersenne***.

1. Montrer que si M_n est premier alors n est premier.
2. Soit p un nombre premier. Montrer que tous les diviseurs (premiers) de M_p sont congrus à 1 modulo p.

Exercice 4 – Étant donné un entier $n > 0$, l'entier $F_n = 2^n + 1$ est le ***n-ème nombre de Fermat***.

1. Montrer que si F_n est premier alors n est une puissance de 2.
2. Supposons que $n > 1$ est une puissance de 2. Montrer que si l'enier F_n divise $3^{n/2} + 1$ alors il est premier. En fait, la réciproque de cette propriété est égaliement vraie. Le critère de primalité pour les nombres de Fermat ainsi obtenu est appelé ***test de Pépin***.

Exercice 5

1. Montrer que pour tout entier $n > 2$, l'entier $\varphi(n)$ est pair.
2. Quelles conditions doit vérifier n pour que $\varphi(n)$ soit congru à 2 modulo 4 (resp. une puissance de 2) ?

Exercice 6 – Montrer que pour tout entier naturel n, on a l'identité

$$\sum_{(n,m)=1, 0 \leq m < n} m = \frac{1}{2} n \varphi(n).$$

Exercice 7 – Soient n et m deux entiers premiers entre eux.

1. Montrer que l'entier nm divise $n^{\varphi(m)} + m^{\varphi(n)} - 1$.

2. Considérons deux entiers a et b. Vérifier que l'entier $x = a + (b-a)n^{\varphi(m)}$ est une solution du système de congruences

$$\begin{cases} x \equiv a \pmod{n}, \\ x \equiv b \pmod{m} \end{cases}$$

Exercice 8 – Soient a et b deux entiers premiers entre eux. En partant d'une identité de Bézout $au + bv = 1$, déterminer une identité de Bézout $a^2n + bm = 1$. En déduire que $(a^2, b) = 1$, puis que $(a^n, b^m) = 1$ quels que soient $n, m \in \mathbb{N}$.

Exercice 9 – Dans cet exercice, on fixe un nombre premier impair p et on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. Considérons l'homomorphisme $f : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ d'élévation au carré. Son image, notée $(\mathbb{F}_p^\times)^2$ est le ***sous-groupe des carrés*** de $\mathbb{F}_p^\times$.

1. Vérifier que $\ker(f) = \{\pm 1\}$. En déduire que $(\mathbb{F}_p^\times)^2$ est d'ordre $(p-1)/2$.
2. Montrer le ***théorème d'Euler***, qui affirme que $x \in \mathbb{F}_p^\times$ appartient à $(\mathbb{F}_p^\times)^2$ si et seulement si $x^{(p-1)/2} = 1$ (indication : on utilisera le fait que le nombre de racines dans $\mathbb{F}_p$ qu'un polynôme non nul $f \in \mathbb{F}_p[X]$ est majoré par $\deg(f)$).
3. En déduire que -1 est un carré dans $\mathbb{F}_p$ si et seulement si p est congru à 1 modulo 4.
4. Montrer que si $x \in \mathbb{F}_p^\times$ n'appartient pas à $(\mathbb{F}_p^\times)^2$ alors $x^{(p-1)/2} = -1$.

Exercice 10– Soit p un nombre premier impair. Le but de cet exercice est de montrer le ***théorème des deux carrés de Fermat*** qui affirme que p est la somme de deux carrés si et seulement s'il est congru à 1 modulo 4.

1. Montrer que si p est la somme de deux carrés alors il est congru à 1 modulo 4.

Réciproquement, soit p congru à 1 modulo 4. D'après l'exercice précédent, -1 est un carré modulo p. Fixons alors un entier w tel que $w^2 \equiv -1 \pmod{p}$, notons m la partie entière de $\sqrt{p}$, i.e. le plus petit entier naturel tel que $n^2 \leq p$ et considérons l'ensemble $S = \{0, 1, \ldots, m\}$.

2. Montrer que l'application $f : S \times S \to \mathbb{F}_p$ qui associe au couple (u, v) la classe de congruence de l'entier $u + vw$ modulo p n'est pas injective (indication : on comparera les cardinaux).
3. Soient (u, v) et (u', v') deux éléments de $S \times S$ tels que $f(u, v) = f(u', v')$ (cf. le point précédent) et posons $a = |u - u'|$ et $b = |v - v'|$. Montrer que l'entier $a^2 + b^2$ est divisible par p. En déduire l'identité $p = a^2 + b^2$.

Exercice 11 – Soit K un corps tel que le groupe $K^\times$ possède un élément x d'ordre 8. Le but de cet exercice est de montrer que 2 est un carré dans K.

1. Vérifier que l'on a l'identité $x^2 + x^{-2} = 0$.
2. Considérons l'élément $y = x + x^{-1}$. En déduire l'identité $y^2 = 2$.
3. Soit p un nombre premier congru à 1 modulo 8. En admettant que le groupe multiplicatif d'un corps fini est cyclique, en déduire que 2 est un carré dans $\mathbb{F}_p$.

Exercice 12 – Soit g un élément d'ordre fini d'un groupe G et notons d non ordre. Montrer que pour tout entier n, l'élément g^n est d'ordre $d/(n, d)$.

Exercice 13 – Soit $G = \{g_1, \ldots, g_n\}$ un groupe abélien fini d'ordre n. Dans la suite, on note $\langle g \rangle$ le sous-groupe engendré par un élément $g \in G$.

1. Quel est l'ordre du groupe $H = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$?

2. Justifier le fait que l'application $f : H \to G$ définie par $f(x_1, \ldots, x_n) = x_1 \cdots x_n$ est un homomorphisme surjectif de groupes. En déduire que n divise l'ordre de H.
3. Montrer que ***théorème de Cauchy*** qui affirme que si p est un nombre premier divisant n alors G possède un élément d'ordre p.