Université Paris 7 - Denis Diderot — 2018-2019
UFR de Mathématiques — M1 - Arithmétique

Feuille d'exercices 3

Le nombre p désigne un nombre premier impair.

Symbole de Legendre

Exercice 1 1. Calculer les symboles de Legendre suivants : $\left(\frac{-1}{17}\right)$, $\left(\frac{2}{29}\right)$, $\left(\frac{13}{17}\right)$, $\left(\frac{7}{19}\right)$, $\left(\frac{-8}{23}\right)$.

2. 2015 est-il un carré modulo 7 ? Modulo 11 ? Modulo 61 ? Modulo 77 ?

Exercice 2 Lemme de Gauss.

Soit $a \in \mathbb{F}_p^\times$. On considère un sous-ensemble $S \subset \mathbb{F}_p^\times$ et on note $aS := \{ax : x \in S\}$. On suppose que les sous-ensembles S et $-S = (-1)S$ forment une partition de $\mathbb{F}_p^\times$.

a) Vérifier que l'ensemble $S_0 = \{1, 2, \cdots, \frac{p-1}{2}\}$ satisfait à cette hypothèse.

b) Montrer que les sous-ensembles aS et $-aS$ forment aussi une partition de $\mathbb{F}_p^\times$.

c) On note $u(a) = \#(S \smallsetminus aS)$ ($S \smallsetminus aS$ désigne S privé de aS).
Montrer l'égalité $\prod_{x\in S} ax = (-1)^{u(a)} \prod_{x\in S} x$.

d) En déduire la formule $a^{(p-1)/2} = (-1)^{u(a)}$.

e) En déduire que 2 est un résidu quadratique modulo p si et seulement si $p \equiv \pm 1 \bmod 8$.

Exercice 3 Déterminer les corps finis dans lesquels 3 est un carré.

Exercice 4 1. Déterminer $\left(\frac{x}{p}\right)$ lorsque x est un générateur de $\mathbb{F}_p^\times$.

2. On suppose que $\frac{p-1}{2}$ est premier. Montrer que $a \in \mathbb{Z}$ est une racine primitive modulo p si, et seulement si, $\left(\frac{a}{p}\right) = -1$ et $a \not\equiv \pm 1 \bmod p$.

Exercice 5 Dénombrer les morphismes de groupes de $\mathbb{F}_p^\times$ dans $\{\pm 1\}$.

Exercice 6 Soient $m, n \in \mathbb{Z}$ avec n impair positif. Montrer que si le symbole de Jacobi $\left(\frac{m}{n}\right)$ vaut -1 alors m n'est pas un carré modulo n.

Exercice 7 Soient $a, b \in \mathbb{Z}$ et $D := a^2 - 4b$. Montrer que l'image du polynôme $X^2 + aX + b$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ est irréductible si et seulement si on a $\left(\frac{D}{p}\right) = -1$. Quoi dire si $p = 2$?

Exercice 8 On se propose de calculer $\left(\frac{-3}{p}\right)$ sans utiliser la loi de réciprocité quadratique.

1. Montrer que $(\mathbb{Z}/p\mathbb{Z})^*$ admet un élément d'ordre 3 si, et seulement si, $p \equiv 1 \bmod 3$.
2. Conclure en considérant le polynôme $X^2 + X + 1$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

Exercice 9 On suppose $p \equiv 1 \bmod 4$. Montrer $\left(\frac{p-1}{2}\right)!^2 \equiv -1 \bmod p$.

Exercice 10

1. Montrer qu'au moins l'un des entiers -1, 2 ou -2 est un carré modulo p.
2. En déduire que le polynôme X^4+1 est irréductible dans $\mathbb{Q}[X]$ mais réductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

Exercice 11 Montrer que -1 est une puissance 4ème modulo p si, et seulement si, on a $p \equiv 1 \bmod 8$.

Exercice 12 Test de primalité de Solovay-Strassen. Soit n un entier impair positif.

1. Montrer que n est premier si, et seulement si, $x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right) \bmod n$ pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^*$.
2. En déduire que si n n'est pas premier, au moins la moitié des $x \in (\mathbb{Z}/n\mathbb{Z})^*$ vérifient $x^{\frac{n-1}{2}} \not\equiv \left(\frac{x}{n}\right) \bmod n$.

Exercice 13 Théorème de Frobenius-Zolotarev. Soit V un $\mathbb{F}_p$-espace vectoriel de dimension finie $n \geqslant 3$. Pour tout $g \in \mathrm{GL}_{\mathbb{F}_p}(V)$, on note $\varepsilon(g)$ la signature de g en tant que bijection de V.

a) On prend ici $V = \mathbb{F}_{p^n}$, on fixe a un générateur de $\mathbb{F}_{p^n}^*$ et on définit $g \in \mathrm{GL}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ par $g(x) = ax$. Déterminer $\varepsilon(g)$.

b) Sachant que $\mathrm{GL}_{\mathbb{F}_p}(V)$ a pour groupe dérivé $\mathrm{SL}_{\mathbb{F}_p}(V) := \{g \in \mathrm{GL}_{\mathbb{F}_p}(V) : \det(g) = 1\}$, montrer que pour tout $g \in \mathrm{GL}_{\mathbb{F}_p}(V)$, on a $\varepsilon(g) = \left(\frac{\det(g)}{p}\right)$.

Exercice 14 Soit $a \geqslant 1$ un entier. Pour tout entier $n \geqslant a$, on considère $b_n = \frac{n!^2}{a} - 1$.

a) Montrer que tout nombre premier p divisant b_n vérifie $p > n$ et $\left(\frac{a}{p}\right) = 1$.

b) En déduire qu'il existe une infinité de nombre premiers p tels que $\left(\frac{a}{p}\right) = 1$.

Exercice 15 Soit n un entier de la forme $n = 1 + 2^m h$ avec m et h entiers tels que $m \geqslant 2$ et $0 < h < 2^m$.

Soit p tel que n n'est pas un résidu quadratique modulo p.

On veut montrer que n est premier si et seulement si $p^{\frac{n-1}{2}} \equiv -1 \bmod n$.

a) Montrer que, si n est premier, cette congruence est bien vérifiée.

b) Ici, on suppose réciproquement que $p^{\frac{n-1}{2}} \equiv -1 \bmod n$ et le but est de montrer que n est premier.

Soit ℓ un nombre premier divisant n. En étudiant l'ordre de la classe de p dans $\mathbb{F}_\ell^\times$, montrer que ℓ est de la forme $\ell = 1 + 2^m h'$.

Conclure.

c) En déduire que le n^{e} nombre de Fermat $F_n = 2^{2^n} + 1$ ($n \geqslant 1$) est premier si et seulement si F_n divise $3^{\frac{F_n-1}{2}} + 1$.