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

Feuille d'exercices 5

Applications du symbole de Legendre

Exercice 1 Soit $\mathcal{C}$ la courbe d'équation $y^2 = x^3 - x$. Étant donné un nombre premier p, on s'intéresse au nombre de points de cette courbe sur $\mathbb{F}_p$, $N_p = \text{card}\{(x,y) \in (\mathbb{F}_p)^2 \mid y^2 = x^3 - x\}$.

a) Montrer la formule $N_p = p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3-x}{p}\right)$.

b) Calculer N_7.

c) Généraliser aux premiers p tels que $p \equiv 3 \bmod 4$.

Exercice 2 Soient $p \geqslant 3$ un nombre premier.

a) Montrer que $x \mapsto \frac{1+x}{1-x}$ induit une bijection de $\mathbb{F}_p \smallsetminus \{1\}$ sur $\mathbb{F}_p \smallsetminus \{-1\}$.

b) En déduire l'égalité $\sum_{x \in \mathbb{F}_p} \left(\frac{1-x^2}{p}\right) = (-1)^{\frac{p+1}{2}}$.

c) Quel est le nombre de points du cercle unité, d'équation $x^2 + y^2 = 1$, sur $\mathbb{F}_p$?

Exercice 3 Calculer le nombre $N(a,b,p)$ de solutions $(x,y) \in (\mathbb{F}_p)^2$ de l'équation $ax^2 + by^2 = 1$.

Exercice 4

1. Si p est premier et $a \in \mathbb{Z}$, on pose $N(a,b) = \text{card}\{(x,y,z) \in (\mathbb{F}_p)^3 \mid x^2+y^2+z^2 \equiv a \bmod p\}$. Lorsque p est impair, montrer que $N(a,b) = p^2 + \left(\frac{-a}{p}\right) p$. Que vaut $N(a,2)$?
2. Soit p premier impair, calculer $N(7,p)$, en supposant $N(p,7) = 42$.
3. Soit p premier impaire tel que $p \equiv 3 \bmod 4$ calculer

$$\text{card}\{(x,y,z) \in (\mathbb{F}_p)^3 \mid x^4 + y^4 + z^4 \equiv 1 \bmod p\}.$$

Exercice 5 On considère la forme quadratique

$$Q(x,y,z,t) = x^2 - 2xy + 3y^2 + 3z^2 + 7t^2.$$

Combien de solution l'équation $Q(x,y,z,t) = 0$ a-t-elle modulo 5 ? Même question modulo 7.

Exercice 6 On se propose de montrer que l'équation

$$2y^2 = x^4 - 41$$

ne possède pas de solutions avec $x, y \in \mathbb{Q}$, et d'évaluer le nombre N_p de solutions dans $\mathbb{F}_p$ pour certains p.

1. Supposons qu'il existe $x = a/b$, $y = c/d$ formant une solution, avec $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}^*$ et $\text{pgcd}(a,b) = \text{pgcd}(c,d) = 1$. Montrer que b^4 divise d^2 et que d^2 divise $2b^4$ et en déduire que $d = b^2$. On obtient donc des entiers a, b, c premiers entre eux tels que
$$2c^2 = a^4 - 41b^4.$$

2. Quel est le cardinal de $\mathbb{F}_{41}^{*2}$, de $\mathbb{F}_{41}^{*4}$? Vérifier que 2 est d'ordre 20 dans $\mathbb{F}_{41}^*$, que 2 est un carré dans $\mathbb{F}_{41}^*$ mais n'est pas un bicarré (puissance quatrième).
3. Soit p premier impair divisant c. Montrer que p est un carré modulo 41. En déduire que c est lui même un carré modulo 41.
4. Montrer que l'existence de $x, y \in \mathbb{Q}$ vérifiant $2y^2 = x^4 - 41$ entraîne que 2 serait un bicarré dans $\mathbb{F}_{41}^*$ et conclure.
   Soit maintenant p un nombre premier différant de 2 et de 41.
5. Rappeler combien des solutions $(x, y, z) \in (\mathbb{F}_p)^3$ possède l'équation $2y^2 = x^2 - 41z^2$. On note L_p ce nombre.
6. Soit M_p le nombre de couples $(x, y) \in (\mathbb{F}_p)^2$ tels que $2y^2 = x^2 - 41$ et soit R_p le nombre de couples $(x, y) \in (\mathbb{F}_p)^2$ tels que $2y^2 = x^2$. Montrer que $L_p = (p-1)M_p + R_p$.
7. Calculer R_p (on distinguera suivant que 2 est un carré modulo p ou non) et en déduire le calcul de M_p.
8. Soit N_p le nombre de couples $(x, y) \in (\mathbb{F}_p)^2$ tels que $2y^2 = x^4 - 41$. Lorsque $p \equiv 3 \bmod 4$, montrer que $N_p = M_p$ et ainsi que

$$N_p = \begin{cases} p+1 \text{ si } p \equiv 3 \bmod 8 \\ p-1 \text{ si } p \equiv 8 \bmod 8 \end{cases}$$

Exercice 7 On se propose de calculer, pour chaque premier $p \neq 2, 17$, le nombre $N_p = \text{card}\{(x, y) \in (\mathbb{F}_p)^2 \mid 2y^2 = x^4 - 17\}$.

1. Calculer les nombres $L_p = \text{card}\{(x, y, z) \in (\mathbb{F}_p)^3 \mid 2y^2 = x^2 - 17z^2\}$ et en déduire le calcul de $M_p = \text{card}\{(x, y) \in (\mathbb{F}_p)^2 \mid 2y^2 = x^2 - 17\}$.
2. Lorsque $p \equiv 3 \bmod 4$, montrer que $N_p = M_p$, et, par conséquent, que

$$N_p = \begin{cases} p+1 \text{ si } p \equiv 3 \bmod 8 \\ p-1 \text{ si } p \equiv 8 \bmod 8 \end{cases}$$

3. On pose

$$\tau(a) = \sum_{x \in \mathbb{F}_p} e^{\frac{ax^2}{p}} \text{ et } \rho(a) = \sum_{x \in \mathbb{F}_p} e^{\frac{ax^4}{p}}.$$

   Monter que

$$N_p = p + p^{-1} \sum_{a=1}^{p-1} e^{\frac{17a}{p}} \tau(2a)\rho(-a).$$

   On suppose désormais $p \equiv 1 \bmod 4$. On introduit $G = \{\chi_0, \chi_1, \chi_2, \chi_3\}$ l'ensemble des caractères de $\mathbb{F}_p^*$ tels que $\chi_0(x) = 1$ et $\chi^4(x) = 1$ pour $x \in \mathbb{F}_p^*$. On les prolonge à $\mathbb{F}_p$ par la convention $\chi_0(0) = 1$ et $\chi_j(0) = 0$ pour $j = 1, 2, 3$. On supposera que χ_1 est le caractère de Dirichlet $\chi_1(x) = \left(\frac{x}{p}\right)$. On introduit aussi les sommes de Gauss associées :

$$G(\chi, a) = \sum_{x \in \mathbb{F}_p} \chi(x) e^{\frac{ax}{p}} \text{ et } G(\chi) = G(\chi, 1).$$

4. Rappeler pourquoi $G(\chi_0, a) = 0$, $G(\chi, a) = \bar{\chi}(a)G(\chi)$ et, enfin, que si $\chi \neq \chi_0$ on a $|G(\chi)| = \sqrt{p}$.

5. Montrer la formule

$$\rho(a) = \bar{\chi}_1(a)G(\chi_1) + \bar{\chi}_2(a)G(\chi_2) + \bar{\chi}_3(a)G(\chi_3).$$

6. En déduire une formule pour N_p en terme des sommes de Gauss de la forme

$$N_p = p - \epsilon_0 + \frac{\tau(1)}{p}(\epsilon_1 G(\chi_2)^2 + \epsilon_2 G(\chi_3)^2),$$

où $|\epsilon_i| = 1$.

7. Conclure que $N_p \geq 1$ pour tout $p \neq 2, 17$.

Exercice 8 On se propose de montrer que l'équation

$$2y^2 = x^4 - 17$$

possède des solutions modulo N pour tout N, mais ne possède aucune solution rationnelle sur $\mathbb{Q}$.

1. Supposons qu'il existe $x = a/b$, $y = c/d$ formant une solution, avec $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}^*$ et $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1$. Montrer que b^4 divise d^2 et que d^2 divise $2b^4$ et en déduire que $d = b^2$ et $2c^2 = a^4 - 17b^4$.
2. Soit $p \neq 2$ divisant c. Montrer que p est un carré modulo 17, et en déduire que c lui-même et un carré modulo 17. Conclure que 2 serait un bicarré modulo 17, et obtenir une contradiction.
3. Soit $p \neq 2, 17$. On a montré à l'exercice précédent qu'il existe $u, v \in \mathbb{F}_p^*$ avec $2u^2 = v^4 - 17$. Montre que l'équation étudiée a des solutions modulo p^n pour tout n.
4. Montrer que l'équation a également des solutions modulo 2^n et modulo 17^n, en affinant le raisonnement précédent. (On pourra observer et utiliser que $2 \cdot 5^2 \equiv 2^4 \bmod 17$ et $3^4 - 17 \equiv 0 \bmod 2^6$.)
5. Conclure par le lemme chinois que l'équation $2y^2 = x^4 - 17$ possède des solutions modulo N pour tout N.