Feuille d'exercices 5

Applications du symbole de Legendre

Exercice 1 a) Astuce : $1+\left(\frac{x}{p}\right)$ est le nombre de racines carrées (mod p) de x. Or, pour x fixé, le nb de solutions de l'équation est le nombre de racines carrés de x^3-x. Donc

$$N_p = \sum_{\mathbb{F}_p}\left(1+\left(\frac{x^3-x}{p}\right)\right) = p+\sum_{\mathbb{F}_p}\left(\frac{x^3-x}{p}\right)$$

b) calcul direct

c) Soit $f(x)=x^3-x$, on vérifie que $f(-x)=-f(x)$. On a $f(x)=0$ ssi $x=0,\pm 1$. Pour toutes les autres valeurs, $f(x)$ et $-f(x)$ sont distincts, et puisque $p=3 \mod 4$ l'une exactement de ces valeurs est un carré. Donc la somme $\sum_{\mathbb{F}_p}\left(\frac{x^3-x}{p}\right)$ vaut 0 dans ce cas, donc le nombre de solutions est p.

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

a) Clair. L'inverse est donné par $y \mapsto \frac{y-1}{y+1}$.

b) En utilisant la question précédente, on montre que la somme à calculer se ramène à

$$\sum_{y\neq -1}\left(\frac{y}{p}\right) = -\left(\frac{-1}{p}\right).$$

c) Technique habituelle : compter le nombre de solutions, revient à calculer la somme sur x du nombre de racines carrées de $1-x^2$, càd

$$\sum_{x\in\mathbb{F}_p} 1+\left(\frac{1-x^2}{p}\right).$$

Exercice 3 Trivial si a ou b est zéro. Dans le cas contraire, on a $x^2=\frac{1-by^2}{a}=\frac{b^{-1}-y^2}{ab}$. Comme d'habitude le calcul du nombre de solutions se ramène à calculer

$$p+\sum\left(\frac{\frac{b^{-1}-y^2}{ab}}{p}\right).$$

La somme dans cette formule est égale à

$$\left(\frac{-ab}{p}\right)\sum\left(\frac{y^2+d}{p}\right).$$

avec $d=-b^{-1}$. Comme y apparait seulement sous la forme y^2 dans la formule sous la somme, on peut se ramener à une somme sur les carrés en faisant attention à les compter avec la bonne multiplicité. Donc :

$$\sum\left(\frac{y^2+d}{p}\right) = \sum(1+\left(\frac{y}{p}\right))\left(\frac{y+d}{p}\right)$$

ou le premier facteur est par définition le nombre de racines carrées de y et le 2e la formule qui nous intéresse, débarassée du carré. En développant on a

$$\sum \left(\frac{y+d}{p}\right) + \sum \left(\frac{y}{p}\right)\left(\frac{y+d}{p}\right)$$

et la première somme est zéro. Pour calculer la seconde, remarquons que si $y \neq 0$, alors $\left(\frac{y}{p}\right) = \left(\frac{y^{-1}}{p}\right)$, et si $y = 0$ le terme correspondant est nul. Donc la somme s'écrit finalement

$$\sum_{y \neq 0} \left(\frac{1+y^{-1}d}{p}\right) = 0 - \left(\frac{1}{p}\right) = -1$$

Exercice 4

1. Appliquer la formule du cours.
2. Formule précédente + réciprocité quadratique
3. Le nombre de solutions est le même que pour léquation avec des carrés au lieu de puissances quatrièmes. Si (x, y, z) est une solution de $x^2+y^2+z^2 = 1 \mod p$ c'est aussi le cas de $(\pm x, \pm y, \pm z)$. En supposant pour simplifier que $x, y, z \neq 0$ [1] on peut donc regrouper les solutions par "paquets" de 8 solutions identiques au signe près. Parmi ces 8 solutions, il en existe exactement une telle que x, y, z soient tous les trois des carrés, puisque $p = 3 \mod 4$ (et donc si $a \neq 0$ l'un exactement de a, $-a$ est un carré). Chacun d'eux a deux racines carrés, ce qui produit au total 8 solutions de l'équation $x^4 + y^4 + z^4 = 1 \mod p$.

Exercice 5 Formule du cours

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. Calcul direct.
2. La moitié des éléments inversibles sont des carrés, donc le cardinal de $\mathbb{F}_{41}^{*2}$ est 20. De même, puisque le groupe des inversible est cyclique, et son cardinal divisble par 4, le nombre de puissqnce 4e est 10. Puisque $41 = 1 \mod 8$, 2 est un carré. Si 2 était un bicarré, on aurait $2^{10} = 1 \mod 41$ ce qui est faux.
3. En considérant l'équation ci-dessus modulo p, on voit que 41 est un carré mod p, puis on utilise la réciprocité quadratique pour voir que p est un carré mod 41. Puisque 2 est un carré mod 41, alors chacun des divisuers premiers de c est un carré. Donc *si c est positif* c'est un carré mod 41. Si c est négatif, c'est encore un carré puisque -1 est un carré mod 41 aussi.
4. Puisque c carré mod 41, alors c^2 est un bicarré mod 41, donc l'équation ci-dessus implique que 2 est un bicarré aussi, absurde.

   Soit maintenant p un nombre premier différant de 2 et de 41.
5. Formule du cours.

1. dans le cas contraire, on suit le même raisonnement avec moins de variables

6. Formule du cours.
7. Formule du cours.
8. Argument habituel : si $p = 3 \mod 4$, alors -1 n'est pas un carré mod p, donc pour tout x non nul exactement l'un de x ou $-x$ est un carré, donc $N_p = M_p$.