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 Trivial

Exercice 2 a) On peut écrire $\mathbb{F}_p^\times = \{-\frac{p-1}{2}, \dots, -1, 1, \dots, \frac{p-1}{2}\}$.

b) Multiplier par un élément inversible est une bijection de $\mathbb{F}_p^\times$ dans lui-même.

c) On a $\prod_{x\in S} ax = \prod_{x\in aS} x$. Pour montrer l'égalité il est plus simple de partir du produit $\prod_{x\in S} x$. Pour $x \in aS$, soit $x \in S$ et dans ce cas on le laisse tel quel, soit $x \notin S$, et dans ce cas $-x \in S$ par la question précédente, dans ce cas on remplace x par $-x$ dans le produit, et on rajoute un $-$ devant le produit pour compenser. Formellement :

$$\prod_{x\in S} x = \prod_{x\in aS\cap S} x \times \prod_{x\in S\setminus aS} -(-x) = \prod_{x\in aS\cap S} x \times (-1)^{u(a)} \prod_{x\in S\setminus aS} (-x)$$

d'où le résultat.

d) On a évidemment $\prod_{x\in S} ax = a^{(p-1)/2} \prod_{x\in S} x$. D'après la question précédente ce produit est aussi égal à $(-1)^{u(a)} \prod_{x\in S} x$. Comme $\prod_{x\in S} x \neq 0$ (et qu'on est dans un corps), on en déduit le résultat.

e) Puisque $\left(\frac{2}{p}\right) = 2^{(p-1)/2}$ il suffit de déterminer quand $(-1)^{u(2)} = 1$. On remarque que $u(2)$ n'est autre que le nombre d'entiers impairs compris entre 1 et $(p-1)/2$, et on veut que $u(2)$ soit pair. si N est un entier, le nombre d'entiers impairs entre 1 et N est :
— $N/2$ si N est pair
— $(N+1)/2$ si N est impair.
Ce nombre est donc lui-même pair si
— $N = 0 \mod 4$ si N est pair
— si $N + 1 = 0 \mod 4$ si N impair.
On applique ce résultat à $N = (p-1)/2$ pour déterminer la parité de $u(2)$. Si $(p-1)/2$ pair on obtient $p - 1 = 0 \mod 8$, s'il est impair $p + 1 = 0 \mod 8$.

Exercice 3 Les cas de caracteristique 2 ou 3 sont triviaux, puisque $3 = 1$ et $3 = 0$ respectivement dans ces cas. On commence par le cas $q = p > 3$ premier. On calcule en utilisant la loi de réciprocité quadratique

$$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \left(\frac{p}{3}\right).$$

On obtient donc 1 si et seulement si :
— $p = 1 \mod 4$ et $p = 1 \mod 3$, càd $p = 1 \mod 12$ par le lemme chinois
— $p = -1 \mod 4$ et $p = -1 \mod 3$, càd $p = -1 \mod 12$ (en effet la condition sur p nous dit que -1 n'est pas un carré, on obtient donc bien $(-1)\times(-1) = 1$).

Si p satisfait ces conditions, alors 3 est *a fortiori* un carré dans tout corps de caractéristique p. Dans le cas contraire, alors le polynôme $X^2 - 3$ est irréductible dans $\mathbb{F}_p[X]$, et 3 est un carré dans $\mathbb{F}_{p^2} \cong F_p[X]/(x^2 - 3)$. C'est donc un carré dans tout corps contenant $\mathbb{F}_{p^2}$, càd tout corps de la forme $\mathbb{F}_{p^{2k}}$.

Exercice 4

1. Si a est un générateur, alors les carrés sont essentiellement par définition les a^{2k}, donc a lui-même n'en est pas un. Dit autrement, si a était un carré et si x était l'un de ses racines carrées, alors l'ordre de x serait le double de l'ordre de a ce qui n'est pas possible.
2. Puisque $p \neq 2$ alors (-1) n'est pas un générateur, et 1 n'en est évidemment jamais un. Donc $a \neq 1, -1$ et d'après ce qui précède $\left(\frac{a}{p}\right) = -1$ (dans ce sens on n'utilise pas l'hypothèse sur p).
   Réciproquement, on sait que l'ordre de a divise $p - 1$ (toujours). En utilisant l'hypothèse sur p on sait donc que cet ordre peut être 1, 2, $(p-1)/2$ ou $p - 1$. Dans le premier cas on aurait $a = 1$, dans le second $a = -1$, et dans le 3e a serait un carré puisque $a^{(p-1)/2} = \left(\frac{a}{p}\right)$ ce qui est faux par hypothèse. Donc a est d'ordre $p - 1$, donc c'est un générateur.

Exercice 5 On a évidemment le morphisme trivial qui envoit tous les éléments sur 1. Supposons donc $f : \mathbb{F}_p^\times \to \{\pm 1\}$ non trivial. En particulier f est surjectif, donc son noyau est un sous groupe d'ordre $(p-1)/2$. Or il n'en existe qu'un seul, puisque $\mathbb{F}_p^\times$ est cyclique, donc il existe un unique f non trivial, il y'en a donc deux en tout. Une vision plus concrète : puisque $\mathbb{F}_p^\times$ est cyclique, f est déterminé par l'image de n'importe quel générateur a, et f est non trivial ssi $f(a) = -1$, donc il n'existe qu'un seul tel f.

Exercice 6 Découle de la définition : si $\left(\frac{m}{n}\right) = -1$, alors l'un au moins des $\left(\frac{m}{p}\right)$, p un diviseur premier impair de n, vaut -1, donc m n'est pas un carré modulo p, donc a *fortiori* pas un carré modulo n.

Exercice 7 C'est la formule habituelle, D est le discriminant. Puisque P est de degré 2, il est réductible ssi il a des racines, ce qui est le cas ssi D est un carré.

Exercice 8

1. $\mathbb{F}_p^\times$ est cyclique, donc il contient un élément d'ordre 3 ssi 3 divise son ordre $p - 1$.
2. On a $(X^3 - 1) = (X - 1)(X^2 + X + 1)$, donc les racines de $P = X^2 + X + 1$ (s'il y'en a) sont exactement les éléments d'ordre 3 (ce sont les éléments a différents de 1 qui satisfont $a^3 = 1$, et puisque 3 est premier ces éléments sont d'ordre exactement 3). Donc P est réductible ssi il existe des éléments d'ordre 3 ssi $p = 1 \mod 3$ par la question précédente. Or, le discriminant de P est -3, donc par l'exo précédent P réductible ssi -3 est un carré. Donc -3 est un carré ssi $p = 1 \mod 3$.

Exercice 9 Similaire à la preuve du thm de WIlson dans la feuille 1, qu'on peut aussi utiliser directement : il nous dit que (sans condition sur p) $(p-1)! = -1 \mod p$. Or on a évidemment, en posant $k = (p-1)/2$,

$$(p-1)! = -k \times \cdots \times -1 \times 1 \times \cdots \times k \mod p.$$

En faisant sortit les signes '-' de la première moitié de ce produit et en les passant à droite, on obtient

$$(k!)^2 = -(-1)^k.$$

Si $p = 1 \mod 4$, alors k est pair, donc le membre de droite est -1.

Exercice 10 1. Deux cas : soit -1 est un carré et c'est fini. Soit -1 n'est pas un carré, et dans ce cas si 2 n'est pas un carré alors -2 en est un, et réciproquement. Alternativement, on a

$$\left(\frac{-1}{p}\right)\left(\frac{-2}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{2}{p}\right) = 1$$

donc l'un au moins des 3 vaut 1.

2. Si -1 est un carré et a un de ses racines, alors $X^4 + 1 = (X^2 - a)(X^2 + a)$. Si 2 est un carré et b une de ses racines, on fait apparaitre

$$X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 + 1)^2 - (bX)^2 = (X^2 - bX + 1)(X^2 + bX + 1)$$

et pareil si -2 est un carré.

Exercice 11 Si -1 est un carré alors ses racines sont d'ordre 4. Or on a des éléments d'ordre 4 ssi 4 divise $p - 1$.

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

1. Si p premier, alors la congruence n'est autre que le lemme d'Euler prouvé plus haut. Réciproquement, soit n un nombre composé qui satisfait la condition. Alors n n'a pas de facteur carré (on peut remarquer que n est un nombre de Carmichael, donc en particulier n'a pas de facteur carré d'après ce qu'on a prouvé dans la feuille 2, soit le prouver directement). Soit q un diviseur premier de n, et $k = n/q$. Puisque n n'a pas de facteur carré, q et k sont premiers entre eux. Par le lemme chinois, il existe un entier a tel que :
   — a n'est pas un carré modulo q
   — $a = 1 \mod k$.
   D'une part, on a que

$$\left(\frac{a}{n}\right) = \left(\frac{a}{q}\right)\left(\frac{a}{k}\right) = \left(\frac{a}{q}\right)\left(\frac{1}{k}\right) = -1.$$

   D'autre part, par hypothèse $a^{(n-1)/2} = \left(\frac{a}{n}\right) \mod n$. Puisque k divise n cette égalité est aussi vraie modulo k. Mais le membre de gauche est égal à $1 \mod k$, contradiction.

2. L'ensemble des éléments x qui satisfont la congruence est clairement un sous groupe de $(\mathbb{Z}/n\mathbb{Z})^*$. Si n est composé, on a trouvé au moins un élément qui ne satisfait pas cette congruence, donc c'est un sous-groupe propre (càd ce n'est pas le groupe tout entier). Donc le nombre d'élément qui satisfont cette congruence est un diviseur propre de $\phi(n)$, en particulier ce nombre est inférieur à $n/2$.