Université Paris-Saclay 2022-2023
M1 M.F., Orsay Arithmétique

T.D. 3 : Caractères

Les exercices soulignés sont ceux qui seront corrigés en TD ; ils sont à chercher en priorité.

Exercice 1 On rappelle que $1457 = 31 \cdot 47$ et que 2389 est premier.

1. Déterminer si -1457 est un carré modulo 2389.
2. Quels sont les p premiers tels que 6 est un carré modulo p ?

Exercice 2 (*Transformation de Fourier discrète*) Soit p premier impair. On désigne par $\zeta_p \in \mathbf{C}$ une racine primitive p-ème de 1, et pour tout $a \in \mathbf{F}_p$ on note ψ_a l'application définie sur $\mathbf{F}_p$ par $\psi_a(x) = \zeta_p^{ax}$. Pour toute fonction $f\colon \mathbf{F}_p \to \mathbf{C}$, on pose $\hat{f}(a) = p^{-1} \sum_{t\in\mathbf{F}_p} f(t)\psi_{-a}(t)$. On dit que $\hat{f}\colon \mathbf{F}_p \to \mathbf{C}$ est la transformée de Fourier discrète de f.

1. Montrer que $f = \sum_{a\in\mathbf{F}_p} \hat{f}(a)\psi_a$.
2. Notons f le symbole de Legendre relatif à p ; exprimer $\hat{f}(a)$ en fonction de $g_a = \sum_{x\in\mathbf{F}_p} \left(\frac{x}{p}\right) \zeta_p^{ax}$ et en déduire la valeur de $\sum_{a\in\mathbf{F}_p} g_a$.

Exercice 3 (*Une preuve de la loi de réciprocité quadratique*) Soient p et ℓ deux nombres premiers impairs, et $\mathbf{K}$ un corps dont $\mathbf{F}_p$ est un sous-corps. On suppose qu'il existe dans $\mathbf{K}$ une racine primitive ℓ-ème de l'unité ζ (i.e. $\zeta^\ell = 1$ et $\zeta \neq 1$). On considère la somme (dont on justifiera qu'elle a bien un sens) :

$$S = \sum_{x\in\mathbf{F}_\ell^\times} \left(\frac{x}{\ell}\right) \zeta^x \,.$$

1. Démontrer que l'existence d'un tel corps $\mathbf{K}$ est équivalente à $\ell \neq p$.
2. Montrer que $S^2 = (-1)^{\frac{\ell-1}{2}}\ell$.
3. Montrer que $S^{p-1} = \left(\frac{p}{\ell}\right)$, et en déduire la loi de réciprocité quadratique.
4. Démontrer qu'il existe une extension $\mathbf{L}$ de $\mathbf{F}_p$ contenant une racine primitive 8-ème de 1 notée ω. En calculant α^2 avec $\alpha = \omega + \omega^{-1}$, démontrer que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Exercice 4 Soient m, n des entiers, et p un nombre premier impair tels que $p > n \geq m$. En utilisant l'exercice 2, démontrer que

$$\left|\sum_{t=m}^{n} \left(\frac{t}{p}\right)\right| < \sqrt{p}\log p \,.$$

Exercice 5 (*Primalité des nombres de Fermat*)

1. Soit $n = h2^m + 1$ avec $m \geq 2$ et $h < 2^m$ impair. Soit p un nombre premier impair tel que $\left(\frac{n}{p}\right) = -1$. Montrer que n est premier si et seulement si $p^{\frac{n-1}{2}} \equiv -1 \,(\mathrm{mod}\, n)$.
2. Soit $F_k = 2^{2^k} + 1$ le k-ème nombre de Fermat ($k \geq 1$). Montrer que F_k est premier si et seulement si F_k divise $3^{\frac{F_k-1}{2}} + 1$.

Exercice 6

1. Soit p premier vérifiant $p \equiv 1$ ou $2 \,(\mathrm{mod}\, 4)$. Montrer que si $2p+1$ est premier alors 2 est racine primitive modulo $2p+1$ (i.e. $\langle 2 \rangle = \mathbf{F}_{2p+1}^{\times}$).
2. Soit p premier, $p \equiv 3 \,(\mathrm{mod}\, 4)$. Montrer que $2p+1$ est premier si et seulement si $2^p \equiv 1 \,(\mathrm{mod}\, 2p+1)$.
3. On note $M_p = 2^p - 1$ le p-ème *nombre de Mersenne*. Montrer que M_{11}, M_{23} et M_{83} ne sont pas premiers.

Exercice 7 (*Primalité des nombres de Mersenne*) Soit p un nombre premier impair. Le p-ème nombre de Mersenne est l'entier $M_p = 2^p - 1$.

On appelle *suite de Lucas–Lehmer* la suite d'entiers $(s_i)_{i \geq 0}$ définie par

$$s_0 = 4\,, \qquad s_{i+1} = s_i^2 - 2\,,\ i \geq 0\,.$$

Le but de cet exercice est de montrer : M_p est premier si et seulement si $s_{p-2} \equiv 0 \,(\mathrm{mod}\ M_p)$.

1. Commencer par vérifier que pour tout i, on a $s_i = \omega^{2^i} + \bar{\omega}^{2^i}$ où $\omega = 2 + \sqrt{3}$ et $\bar{\omega} = 2 - \sqrt{3}$. Supposons maintenant $s_{p-2} \equiv 0 \,(\mathrm{mod}\, M_p)$.
   (a) Montrer qu'il existe un entier k tel que $\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1$. Par l'absurde, on suppose désormais M_p composé. Notons q le plus petit facteur premier de M_p.
   (b) Justifier l'existence d'un morphisme d'anneaux $\varphi : \mathbf{Z}[\sqrt{3}] \to \mathbf{F}_q[t]/(t^2-3)$. Montrer que $\varphi(\omega)$ est d'ordre 2^p dans le groupe des inversibles de $\mathbf{F}_q[t]/(t^2-3)$.
   (c) Déduire une contradiction.
2. Réciproquement supposons M_p premier.
   (a) Montrer que 3 est un non-carré modulo M_p et que 2 est un carré modulo M_p.
   (b) Notons $\sigma = 2\sqrt{3}$ dans le corps $\mathbf{F}_{M_p}(\sqrt{3})$. Montrer que $(6+\sigma)^{M_p} = 6 - \sigma$.
   (c) Notons $\alpha = (6+\sigma)^2/24$. Montrer que $\alpha^{\frac{M_p+1}{2}} = -1$ et faire le lien entre α et ω.
   (d) Conclure que $s_{p-2} \equiv 0 \,(\mathrm{mod}\, M_p)$.

Ce test particulièrement efficace explique pourquoi les plus grands nombres premiers connus sont des nombres de Mersenne.

Exercice 8 Calculer le symbole de Jacobi $\left(\frac{401}{12869}\right)$; on rappelle que $12869 = 17 \cdot 757$.

Exercice 9 Soient $a, b, c \in \mathbf{Z}$ et p premier tels que $p \equiv 1 \pmod 4$ et $p \nmid abc$. On note A_p le nombre de solutions modulo p de l'équation $aX^4 + bY^4 = c$. En utilisant les sommes de Jacobi, montrer que $|A_p - p| < 3 + 6\sqrt{p}$; en déduire que $A_p > 0$ dès que $p \geq 43$.

Exercice 10 (*Test de primalité de Solovay–Strassen*)

1. Donner un exemple d'entier impair positif n ayant exactement deux facteurs premiers distincts, tel qu'il existe $a \in \mathbf{Z}$ premier avec n vérifiant $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod n$.
2. Dans le reste de l'exercice on étudie le test de primalité probabiliste suivant, dû à Solovay et Strassen. Soit n impair. On choisit $a \in \{1, \ldots, n-1\}$; on teste si $a \wedge n = 1$ et si $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n$. Si l'une de ces deux propriétés est fausse, l'entier a a permis de détecter que n n'est pas premier. Sinon, on recommence avec un autre entier a. On pose $G = \left\{a \in (\mathbf{Z}/n\mathbf{Z})^\times ; \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n\right\}$ et on suppose que n est impair et composé. On va montrer que $G \neq (\mathbf{Z}/n\mathbf{Z})^\times$.
   Justifier que ceci suffit pour déduire qu'au moins la moitié des $a \in (\mathbf{Z}/n\mathbf{Z})^\times$ permettent de détecter la non-primalité de n.
3. Le but de cette question est de montrer par l'absurde que $G \neq (\mathbf{Z}/n\mathbf{Z})^\times$ *dans le cas où n est composé, impair et sans facteur carré.* Supposons donc que $G = (\mathbf{Z}/n\mathbf{Z})^\times$.
   (a) Justifier que $a^{\frac{n-1}{2}} \equiv \pm 1 \pmod n$ pour tout entier a premier à n.
   (b) On fixe un entier a premier à n. Justifier l'existence d'un entier b premier à n et d'entiers premiers entre eux $r \geq 3$, $s \geq 3$ satisfaisant
   $$n = rs\,, \qquad b \equiv 1 \pmod r\,, \qquad b \equiv a \pmod s\,.$$
   En déduire que l'on a en fait $a^{\frac{n-1}{2}} \equiv 1 \pmod n$ pour tout a premier à n.
   (c) Justifier l'existence d'un nombre premier p, d'un entier q non multiple de p et d'un entier a_0 tels que $n = pq$ et $\left(\frac{a_0}{n}\right) = -1$. Conclure.
4. Dans cette question on traite le cas où n est composé, impair, mais admet un facteur carré.
   (a) Soit p un nombre premier impair et $i \geq 1$ un entier. Montrer que, pour tout $a \in \mathbf{Z}$:
   $$(p \nmid a) \Rightarrow \left(\exists b \in \mathbf{Z},\, p \nmid b,\, (1 + p^i a)^p = 1 + p^{i+1} b\right)\,.$$
   (b) Soit p un nombre premier impair et $e \geq 2$ un entier. Montrer que le sous-groupe H de $(\mathbf{Z}/p^e\mathbf{Z})^\times$ formé des éléments congrus à 1 modulo p est cyclique de cardinal p^{e-1} et engendré par la classe de tout élément de la forme $1 + pa$, avec $p \nmid a$.
   (c) Écrivons $n = p^e q$, où $e \geq 2$ et p est premier impair et ne divise pas q. Supposons que $G = (\mathbf{Z}/n\mathbf{Z})^\times$. Montrer alors que l'exposant du groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ (i.e. le ppcm des ordres de ses éléments) divise $n - 1$, et en déduire une contradiction en utilisant (b).

Exercice 11 Soient $a_1, \dots, a_n$ des entiers, $r_1, \dots, r_n$ des entiers strictement positifs, et p un nombre premier tel que $p \nmid a_1 \cdots a_n$. On note $N(p)$ le nombre de n-uplets $(x_1, \dots, x_n) \in \mathbf{F}_p^n$ tels que $a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n} = 0$. Le but de cet exercice est de montrer que $|N(p) - p^{n-1}| \leq C(p-1)p^{\frac{n}{2}-1}$, où $C = (d_1 - 1)(d_2 - 1)\cdots(d_n - 1)$ et pour tout i, $d_i = \operatorname{pgcd}(r_i, p-1)$.

1. Soit $F \in \mathbf{F}_p[X_1, \dots, X_n]$. Montrer que
$$\#\{(x_1, \dots, x_n) \in \mathbf{F}_p^n \colon F(x_1, \dots, x_n) = 0\} = p^{-1} \sum_{y, y_1, \dots, y_n \in \mathbf{F}_p} e\left(\frac{yF(y_1, \dots, y_n)}{p}\right),$$
où l'on note $e(z) = \exp(2i\pi z)$.
2. Montrer que pour tout $a \in \mathbf{Z}$ non multiple de p et tout $r \geq 1$, on a
$$\sum_{y \in \mathbf{F}_p} e\left(\frac{ay^r}{p}\right) = \sum_{\substack{\chi^d = 1 \\ \chi \neq 1}} G(\chi, a)$$
où $d = \operatorname{pgcd}(r, p-1)$, $G(\chi, a) = \sum_{x \in \mathbf{F}_p} \chi(x)\zeta_p^{ax}$ et $\zeta_p = e(1/p)$.
3. Conclure. Qu'obtient-on si $C = 0$, et comment peut-on le démontrer facilement dans ce cas ?

Exercice 12 On note α l'unique caractère de Dirichlet modulo 4 non trivial ; il est donné par $\alpha(n) = (-1)^{\frac{n-1}{2}}$ si n est impair. On considère $\beta : \mathbf{Z} \to \mathbf{R}$ défini par $\beta(n) = (-1)^{\frac{n^2-1}{8}}$ si n est impair, $\beta(n) = 0$ sinon.

1. Montrer que β est un caractère de Dirichlet modulo 8.
2. Soit $a > 1$ impair sans facteur carré. Si n est premier à $4a$, on pose $\chi_a(n) = \alpha(n)^{\varepsilon(a)} \left(\frac{n}{a}\right)$, où $\left(\frac{n}{a}\right)$ désigne le symbole de Jacobi et ε est le prolongement aux entiers impairs de l'unique isomorphisme $(\mathbf{Z}/4\mathbf{Z})^\times \to \mathbf{Z}/2\mathbf{Z}$. Si $\operatorname{pgcd}(n, 4a) \neq 1$ on pose $\chi_a(n) = 0$.
   (a) Montrer que l'application χ_a est un caractère de Dirichlet modulo $4a$.
   (b) Montrer que pour tout p premier ne divisant pas $4a$, on a $\chi_a(p) = 1$ si et seulement si a est un carré modulo p. En déduire que χ_a est non trivial.
3. Soit $a \in \mathbf{Z}$ un entier impair sans facteur carré. Montrer qu'il existe un caractère de Dirichlet χ modulo $4|a|$ tel que pour tout p premier ne divisant pas $4a$ on a $\chi(p) = 1$ si et seulement si a est un carré modulo p. Faire de même pour $a = 2$.

Exercice 13 On considère l'équation (E) : $x^4 - 17 = 2y^2$.

1. Montrer que l'équation $x^4 - 17z^4 = 2y^2$ n'admet pas de solution entière avec $z \neq 0$ et en déduire que (E) n'admet pas de solution rationnelle.
2. Montrer que (E) admet des solutions modulo tout nombre premier p (en utilisant l'exercice 9 si $p \equiv 1 \pmod 4$ et $p \geq 43$, et en traitant directement les autres cas).