Université Paul Sabatier
Licence L3 ESR 2017–2018
Arithmétique

TD 4 : Résidus quadratiques.

Exercice 1. Soient un nombre premier $p > 2$ et a, b, c trois entiers, avec a et b non divisibles par p. Montrer qu'il existe des entiers x, y tels que $ax^2 + by^2 \equiv c \bmod p$. (Indication : combien y a-t-il de carrés dans $\mathbb{Z}/p\mathbb{Z}$?)

Exercice 2. Soient p un nombre premier congru à 3 modulo 4 et a un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$. Exprimer en fonction de a et p les deux racines carrées de a.

Exercice 3. Que donne le lemme de Gauss pour $a = -1$?

Exercice 4. Soit p un nombre premier congru à 1 modulo 4. Montrer que la somme des entiers compris entre 1 et $p-1$ qui sont des carrés mod$p$ est égale à $p(p-1)/4$. (Indication : $a + (p-a) = p$.)

Exercice 5. Soit un nombre premier $p > 2$.

1) Démontrer le théorème de Wilson : $(p-1)! \equiv -1 \bmod p$.
2) En déduire que le produit des carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$ est égal à $(-1)^{(p+1)/2} \pmod p$. (Indication : $k(p-k) \equiv -k^2$.)

Exercice 6. Soient $p = 1 + mn$ un nombre premier et a un entier non divisible par p.

1) Montrer que a est une puissance n-ième mod$p$ si (et seulement si) $a^m \equiv 1 \bmod p$.
2) Pour $n = 2$ (donc $p \neq 2$), en déduire le "critère d'Euler" usuel : $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p$.

Exercice 7. Montrer que pour tout nombre premier $p \equiv 3 \bmod 4$, si $p' = 2p + 1$ est premier alors $2^p \equiv 1 \bmod p'$. En déduire que le nombre de Mersenne $2^{251} - 1$ n'est pas premier.

Exercice 8. Soient p premier impair et $\varepsilon := \begin{cases} 1 \text{ si } p \equiv \pm 1 \bmod 8 \\ -1 \text{ si } p \equiv \pm 3 \bmod 8 \end{cases}$. On se propose de redémontrer que $\left(\frac{2}{p}\right) = \varepsilon$ par une méthode voisine (en plus simple) de celle vue en cours pour le théorème fondamental. On considère pour cela, dans l'anneau $\mathrm{F}_p[\zeta] := \mathrm{F}_p[X]/\left(X^4 + 1\right)$, l'élément $\tau := \zeta + \zeta^{-1}$. Démontrer que :

1) $\tau^2 = 2$;
2) $\left(\frac{2}{p}\right) = \tau^{p-1}$;
3) τ est inversible ;
4) $\tau^p = \varepsilon\tau$ (indication : remarquer que $\tau^p = \zeta^p + \zeta^{-p}$).
5) Conclure.

Exercice 9. Le but de cet exercice est de déterminer les carrés modulo les *puissances* d'un nombre premier *impair*.

1) Soient P un polynôme à coefficients entiers, p un nombre premier, k un entier positif, et $r \in \mathbb{Z}$ tel que $P(r) \equiv 0 \bmod p^k$ et $P'(r) \not\equiv 0 \bmod p$. Montrer qu'il existe un entier $s \equiv r \bmod p^k$ tel que $P(s) \equiv 0 \bmod p^{2k}$.
2) En déduire que si p est impair, tout entier non divisible par p qui est un carré mod$p$ est aussi un carré modp^m pour tout $m \in \mathbb{N}^*$.
3) Ce n'est pas aussi simple si $p = 2$: trouver un entier impair qui est un carré mod2 mais pas mod4, et un entier impair qui est un carrémod4 mais pas mod8.

Exercice 10. Le but de cet exercice est de déterminer les carrés modulo les puissances de 2. Soit un entier $r \geq 3$.

1) Quel est l'ordre du groupe multiplicatif $(\mathbb{Z}/2^r\mathbb{Z})^\times$?
2) Trouver le nombre de carrés dans ce groupe, en considérant les carrés des entiers impairs compris entre 0 et 2^{r-2}.
3) Vérifier que tout carré impair est congru à 1 mod 8.
4) En déduire quels sont les carrés dans $(\mathbb{Z}/2^r\mathbb{Z})^\times$.

5) (facultatif) Et dans $\mathbb{Z}/2^r\mathbb{Z}$?

Exercice 11. Soit un nombre premier $p \geq 5$.

1) Déduire de la loi de réciprocité quadratique (jointe à sa première loi complémentaire) que
$$p \equiv 1 \bmod 3 \Leftrightarrow \left(\frac{-3}{p}\right) = 1.$$
La suite de l'exercice va consister à redémontrer directement que $3 \mid p-1$ si et seulement si -3 est un carré modulo p.
2) Montrer que $p \equiv 1 \bmod 3$ si et seulement si le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ contient un élément d'ordre 3.
3) Montrer que les éventuels éléments d'ordre 3 de $(\mathbb{Z}/p\mathbb{Z})^*$ sont exactement les racines dans $\mathbb{Z}/p\mathbb{Z}$ du polynôme X^2+X+1.
4) Conclure.

Exercice 12. Soit p un nombre premier différent de 2 et 5.

1) Déduire de la loi de réciprocité quadratique que
$$p \equiv \pm 1 \bmod 5 \Longleftrightarrow \left(\frac{5}{p}\right) = 1.$$
La suite (facultative) de l'exercice va consister à redémontrer directement que $5 \mid p^2-1$ si et seulement si 5 est un carré mod p. On note F_{p^2} le corps fini à p^2 éléments.
2) Montrer que $5 \mid p^2-1$ si et seulement si le groupe $\left(\mathrm{F}_{p^2}\right)^*$ contient un élément d'ordre 5.
3) Montrer que les éventuels éléments d'ordre 5 de $\left(\mathrm{F}_{p^2}\right)^*$ sont exactement les racines dans F_{p^2} du polynôme $X^4+X^3+X^2+X+1$.
4) Vérifier qu'un élément x est racine de $X^4+X^3+X^2+X+1$ si et seulement si $x \neq 0$ et l'élément $t := x + \frac{1}{x}$ est racine de T^2+T-1.
5) Montrer que si $p \equiv \pm 1 \bmod 5$ et si x est un élément d'ordre 5 de $\left(\mathrm{F}_{p^2}\right)^*$ alors l'élément $t := x + \frac{1}{x}$ appartient non seulement au corps F_{p^2} mais au sous-corps $\mathrm{F}_p := \mathbb{Z}/p\mathbb{Z}$. (Indication : développer $\left(x+\frac{1}{x}\right)^p$.)
6) En déduire que $5 \mid p^2-1$ si et seulement s'il existe $t \in \mathrm{F}_p$ tel que $t^2+t-1=0$.
7) Conclure.

Exercice 13. (Facultatif) Soient p et q deux nombres premiers impairs distincts. On se propose de redémontrer que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

1) Déduire du lemme de Gauss que $\left(\frac{p}{q}\right) = (-1)^l$ où l est le nombre de couples $(x,y) \in \mathbb{Z}^2$ tels que $0 < x < q/2$ et $-q/2 < px - qy < 0$.
2) Montrer qu'un tel couple (x,y) appartient au rectangle $0 < x < q/2$, $0 < y < p/2$.
3) Montrer que de même, $\left(\frac{q}{p}\right) = (-1)^m$ où m est le nombre de points $(x,y) \in \mathbb{Z}^2$ de ce même rectangle tels que $-p/2 < qy - px < 0$.
4) Montrer que $(p-1)(q-1)/4 - (l+m)$ est le nombre de points $(x,y) \in \mathbb{Z}^2$ de ce rectangle vérifiant soit $px - qy \leq -q/2$, soit $qy - px \leq -p/2$, et que ces deux zones sont en bijection.
5) Conclure.

Exercice 14. (Facultatif) Le symbole de Jacobi $\left(\frac{a}{n}\right)$ est défini pour tout $n \in \mathbb{N}$ impair et tout $a \in \mathbb{Z}$ comme produit de symboles de Legendre, en faisant intervenir la décomposition en facteurs premiers de n : pour toute suite finie de nombres premiers impairs p_i (non nécessairement distincts), $\left(\frac{a}{\prod p_i}\right) = \prod_{1 \leq i \leq k} \left(\frac{a}{p_i}\right)$.

1) Montrer que $\left(\frac{a}{n}\right) = \pm 1$ si a et n sont premiers entre eux et que $\left(\frac{a}{n}\right) = 0$ sinon.
2) A-t-on $\left(\frac{a}{n}\right) = -1 \Rightarrow a$ n'est pas un carré mod$n$? A-t-on $\left(\frac{a}{n}\right) = 1 \Rightarrow a$ est un carré mod$n$?
3) Calculer $\left(\frac{123}{917}\right)$.
4) Montrer que (pour p_i impairs) $\prod p_i = \prod (1 + p_i - 1) \equiv 1 + \sum (p_i - 1) \bmod 4$, et en déduire que $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.
5) Montrer de même que (pour $m, n \in \mathbb{N}$ impairs) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}$.
6) Montrer que $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ (indication : $\prod p_i^2 = \prod (1 + p_i^2 - 1) \equiv \ldots \bmod \ldots$).