

## TD 2. Éléments primitifs et résidus quadratiques

### Exercice 1 (Loi de réciprocité quadratique)

- Calculer  $\left(\frac{17}{41}\right)$  et  $\left(\frac{1999}{65537}\right)$ .
- Déterminer à l'aide de la loi de réciprocité quadratique les premiers impairs  $p$  tels que 7 soit un carré modulo  $p$ . Faire de même pour 15.

### Exercice 2 (Éléments primitifs)

On rappelle que si  $p$  est premier, un entier  $a$  est dit *primitif modulo  $p$*  si la classe de  $a$  modulo  $p$  engendre  $(\mathbb{Z}/p\mathbb{Z})^\times$ .

- Quels sont les ordres possibles des éléments de  $(\mathbb{Z}/29\mathbb{Z})^*$  ?
  - Montrer que 2 est un élément primitif modulo 29.
  - Donner la liste des puissances de 2 qui sont des éléments primitifs modulo 29.
  - Résoudre l'équation  $x^7 \equiv 1 \pmod{29}$ .
- Déterminer de même les éléments primitifs modulo 11 et 13.
- Soit  $p$  un premier impair.
  - Soit  $a$  un élément primitif modulo  $p^2$ . Montrer que  $a$  est un élément primitif modulo  $p$ .
  - On suppose  $p$  congru à 1 modulo 4, montrer que  $a$  est un élément primitif modulo  $p$  si et seulement si  $-a$  est un élément primitif modulo  $p$ .  
[Pour ( $\Rightarrow$ ), on pourra considérer un entier  $\ell$  tel que  $(-a)^\ell \equiv 1 \pmod{p}$  et voir ce que cela entraîne pour  $a^\ell$  selon que  $\ell$  est pair ou impair.]
  - On suppose  $p$  congru à 3 modulo 4, montrer que  $a$  est un élément primitif modulo  $p$  si et seulement si  $-a$  est d'ordre  $\frac{p-1}{2}$  dans  $(\mathbb{Z}/p\mathbb{Z})^*$ .  
[Pour ( $\Leftarrow$ ), on établira l'implication :  $\forall \ell \in \mathbb{Z}, a^\ell \equiv 1 \pmod{p} \Rightarrow \frac{p-1}{2} \mid \ell$  et on vérifiera qu'elle entraîne que  $\frac{p-1}{2}$  divise l'ordre de  $a$ .]

### Exercice 3 (Résidus quadratiques)

Soit  $p$  un nombre premier.

- Donner une nouvelle preuve du théorème de WILSON :

$$(p-1)! \equiv -1 \pmod{p} .$$

en utilisant l'existence d'un élément primitif  $a$  modulo  $p$ .

En déduire une formule pour la racine carrée de  $-1$  modulo  $p$  lorsque  $p \equiv 1 \pmod{4}$ .

- Soit  $\mathcal{R}$  l'ensemble des entiers compris entre 1 et  $p-1$  qui sont *résidus quadratiques* modulo  $p$  (c'est-à-dire congrus à un carré modulo  $p$ ).

a) Soit  $a$  un élément primitif modulo  $p$ , montrer que  $\mathcal{R} = \{a^{2n} : 1 \leq n \leq p-1\}$

b) En déduire :

$$\prod_{x \in \mathcal{R}} x \equiv \begin{cases} 1 \pmod{p} & \text{si } p = 2 \text{ ou } p \equiv 3 \pmod{4}, \\ -1 \pmod{p} & \text{sinon.} \end{cases}$$

Qu'en est-il du produit des entiers compris entre 1 et  $p-1$  qui ne sont pas résidus quadratiques modulo  $p$  ?

#### Exercice 4 (Symbole de Legendre)

- a) Soit  $p$  un premier impair avec  $p \equiv 1 \pmod{3}$ , montrer que  $(\mathbb{Z}/p\mathbb{Z})^*$  contient un élément  $x$  d'ordre 3. Vérifier que  $(2x+1)^2 \equiv -3 \pmod{p}$ , en déduire la valeur de  $\left(\frac{-3}{p}\right)$ .
- b) Faire de même quand  $p \equiv 1 \pmod{5}$  (on calculera  $(x+x^4)^2 + (x+x^4) - 1$  modulo  $p$ , où  $x$  est d'ordre 5).

#### Exercice 5 (Sommes de symboles)

Soient  $p$  un nombre premier impair,  $a$  et  $b$  des entiers.

1. a) Vérifier que  $\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) = 0$ ;
- b) en déduire la valeur de  $\sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right)$  en supposant que  $a$  est premier à  $p$ .
2. a) Vérifier que le nombre de solutions modulo  $p$  de  $x^2 \equiv a \pmod{p}$  est égal à  $1 + \left(\frac{a}{p}\right)$ .
- b) En supposant  $a$  premier à  $p$ , en déduire que le nombre de solutions modulo  $p$  de  $ax^2 + bx + c \equiv 0 \pmod{p}$  est égal à  $1 + \left(\frac{b^2 - 4ac}{p}\right)$ .
- c) Montrer que le polynôme  $X^2 + X + 1$  est irréductible dans  $\mathbb{F}_5[X]$ .
3. a) Montrer que le nombre  $N$  de solutions de  $x^2 - y^2 \equiv a \pmod{p}$  est  $p + \sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p}\right)$  (on pourra utiliser 2.a).
- b) Utiliser le changement de variables  $u = x + y$ ,  $v = x - y$  pour trouver une autre expression de  $N$  (on traitera séparément les deux cas  $(a, p) = 1$  et  $p | a$ ).
- c) En déduire que :

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p}\right) = \begin{cases} -1 & \text{si } a \text{ est premier à } p, \\ p-1 & \text{si } p | a. \end{cases}$$

#### Exercice 6 (Théorème Chinois des restes)

1. On rappelle que l'indicateur de Carmichael d'un entier  $n$  est l'exposant de  $(\mathbb{Z}/n\mathbb{Z})^*$ .
- a) Donner la décomposition en facteurs premiers de 561 ;
- b) à l'aide du théorème chinois des restes, en déduire la structure de  $(\mathbb{Z}/561\mathbb{Z})^*$  ;
- c) donner enfin les valeurs de l'indicateur d'Euler  $\varphi(561)$  et de celui de Carmichael  $\lambda(561)$ .
2. Soit  $D$  un entier naturel impair et sans facteur carré.
- a) Montrer qu'il existe  $b \in \mathbb{Z}$  tel que  $\left(\frac{b}{D}\right) = -1$ .
- b) On note  $\varphi = \varphi(D)$  et  $a_1, a_2, \dots, a_\varphi$  des entiers représentant les éléments de  $(\mathbb{Z}/D\mathbb{Z})^*$ . Montrer qu'on a :

$$\sum_{i=1}^{\varphi} \left(\frac{a_i}{D}\right) = 0 .$$

En déduire qu'exactement la moitié des éléments  $a$  de  $(\mathbb{Z}/D\mathbb{Z})^*$  vérifient  $\left(\frac{a}{D}\right) = 1$ .

- c) Soit  $p$  un premier impair avec  $(p, D) = 1$  et  $p \equiv 1 \pmod{4}$ . Montrer que  $\left(\frac{D}{p}\right) = 1$  si et seulement si il existe  $i$  tel que  $p \equiv a_i \pmod{D}$  et  $\left(\frac{a_i}{D}\right) = 1$ .
- d) Qu'en est-il si  $p \equiv 3 \pmod{4}$  ?

#### Exercice 7 (Racines carrées)

Appliquer l'algorithme de Tonelli & Shanks pour déterminer les racines carrées des éléments de  $(\mathbb{Z}/p\mathbb{Z})^\times$  qui sont des carrés dans les cas suivants :

- a)  $p = 13$  ;
- b)  $p = 17$ .

On pourra noter que  $(a \text{ et } b \text{ carrés}) \Rightarrow ab \text{ carré}$ .