

Chapitre 5

Résidus quadratiques

5.1 Résidus quadratiques modulo un premier

Définition 5.1.1. Soit p un nombre premier. Un entier a est un résidu quadratique si et seulement si a est premier avec p et il existe k tel que $k^2 \equiv a \pmod{p}$. Un entier a premier avec p qui n'est pas un résidu quadratique est appelé un non résidu quadratique.

Remarque 5.1.2. Cela ne dépend que de la classe de a modulo p .

Théorème 5.1.3. Soit $p = 2l + 1$ un nombre premier impair.

- a) Les résidus quadratiques modulo p forme un sous-groupe de cardinal l de $(\mathbb{Z}/p\mathbb{Z})^*$.
- b) $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ est un résidu quadratique si et seulement si $\bar{a}^l = \bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$.
- c) -1 est un résidu quadratique modulo p si et seulement si $p \equiv 1 \pmod{4}$.

5.2 Symbole de Legendre

Définition 5.2.1. Soit p est nombre premier, et a un entier. Le symbole de Legendre noté $\left(\frac{a}{p}\right)$ vaut :

- 0 si p divise a ,
- 1 si $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ est un carré (résidu quadratique),
- 1 si $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ n'est pas un carré (non-résidu quadratique).

Remarque 5.2.2. Si $a \equiv b \pmod{p}$, alors $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

- Proposition 5.2.3.**
- a) Pour p premier impair, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
 - b) Pour p premier impair et a premier avec p , $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
 - c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

Théorème 5.2.4 (Réciprocité quadratique). Pour p et q premiers impairs, on a :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & \text{si } p \text{ et } q \text{ sont congrus à } 3 \text{ modulo } 4, \\ 1 & \text{si } p \text{ ou } q \text{ est congru à } 1 \text{ modulo } 4. \end{cases}$$

On pourra trouver une démonstration (d'après Zolotarev) à l'adresse : <http://math.unice.fr/~serman/ recip.pdf>.

5.3 Symbole de Jacobi

On étend le symbole de Legendre au cas de nombres qui ne sont plus nécessairement premiers.

Définition 5.3.1. Si b est le produit des nombres premiers $p_1, \dots, p_m$, alors :

$$\left(\frac{a}{b}\right) = \prod_{j=1}^m \left(\frac{a}{p_j}\right).$$

Proposition 5.3.2. a) $\left(\frac{a}{b}\right) = 0$ si et seulement si $\text{PGCD}(a, b) > 1$.

b) $\left(\frac{1}{c}\right) = 1$, et $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$.

c) Si $a \equiv a' \pmod{b}$, alors $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$.

d) Si a et b sont premiers entre eux et impairs, alors :

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} = \begin{cases} -1 & \text{si } a \text{ et } b \text{ sont congrus à } 3 \text{ modulo } 4, \\ 1 & \text{si } a \text{ ou } b \text{ est congru à } 1 \text{ modulo } 4. \end{cases}$$

$$e) \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{4}} = \begin{cases} 1 & \text{si } b \text{ est congru à } \pm 1 \text{ modulo } 8, \\ -1 & \text{si } b \text{ est congru à } \pm 3 \text{ modulo } 8. \end{cases}$$

5.4 Application aux tests de primalité

5.4.1 Nombres de Fermat

Le n -ième nombre de Fermat est : $F_n = 2^{2^n} + 1$.

Proposition 5.4.1. Si un nombre premier p divise F_n , $n \geq 2$, alors il est de la forme

$$p = k2^{n+2} + 1.$$

Exercice 5.4.2. Soit a un élément d'un groupe G noté multiplicativement, de neutre e . Montrer que s'il existe un nombre premier p et un entier k tels que :

$$a^{p^k} = e, \text{ et } a^{p^{k-1}} \neq e,$$

alors a est d'ordre p^k .

Exercice 5.4.3. Démontrer que si un nombre premier p divise F_n , $n \geq 2$, alors il est de la forme

$$p = k2^{n+2} + 1 .$$

Théorème 5.4.4 (Critère de Pépin). *Le nombre de Fermat F_n , $n \geq 1$, est premier si et seulement si*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n} .$$

5.4.2 Test de Solovay et Strassen

Théorème 5.4.5. *Soit $n > 2$ un entier impair.*

- a) $G_n = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z}, 0 \neq \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}\}$ est un sous groupe de $(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}), \times)$.
- b) Si n est premier, alors : $G_n = (\mathcal{U}(\mathbb{Z}/n\mathbb{Z}), \times)$ est de cardinal $n - 1$.
- c) Si n n'est pas premier, alors G_n est de cardinal inférieur ou égal à $\frac{n-1}{2}$.

Entrée : entier impair n à tester, entier t donnant le nombre de *témoins*.

```

Pour  $i$  de 1 à  $t$  faire
    choisir au hasard  $a$  entre 2 et  $n - 2$ ;
     $p \leftarrow (a^{\frac{n-1}{2}} \pmod{n})$ ;
    Si ( $p \neq 1$  et  $p \neq n - 1$ ) Alors
        | Sortie("non premier");
    Fin Si
     $j \leftarrow \left(\frac{a}{n}\right)$ ;
    Si ( $p \neq (j \pmod{n})$ ) Alors
        | Sortie("non premier");
    Fin Si
Fin Pour
Sortie("très probablement premier");

```

Algorithme 8: Test de Solovay et Strassen

Remarque 5.4.6. En utilisant un algorithme de calcul rapide de puissances, on obtient une complexité $O(t \log(n)^3)$. La probabilité pour qu'un nombre non premier ne soit pas détecté est inférieure à 2^{-t} .