Chapitre 5

Résidus quadratiques

5. Résidus quadratiques modulo un premier

Définition 5. . . 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 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. .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) $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ est un résidu quadratique si et seulement si : $\overline{a}^l = \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$.
c) -1 est un résidu quadratique modulo p si et seulement si $p \equiv 1$ (mod 4).

5.2 Symbole de Legendre

Définition 5.2. . 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 $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ est un carré (résidu quadratique),
-1 si $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ 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, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ (mod 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/∼⊀⊄⊄←←⊀←⊀←{∈←{∈∈←

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*

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

5.4.2 Test de Solovay et Strassen

Théorème 5.4.5. *Soit $n > 2$ un entier impair.*
a) $G_n = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z},\ 0 \neq \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \mod n\}$ 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 $n-2$;
  $p \leftarrow (a^{\frac{n-1}{2}} \bmod n)$;
  Si ($p \neq 1$ et $p \neq n-1$) **Alors**
    Sortie("non premier") ;
  Fin Si
  $j \leftarrow \left(\frac{a}{n}\right)$;
  Si ($p \neq (j \bmod n)$) **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}.