Les résidus quadratiques

1 Racine carrée dans $\mathbb{Z}/p\mathbb{Z}$ (p premier $\neq 2$)

Soit p un nombre premier impair et soit a un entier. Le fait que a soit un carré modulo p ne dépend que de la classe de a modulo p. Nous allons donc nous placer dans le corps $\mathbb{Z}/p\mathbb{Z}$ et étudier les nombres qui sont des carrés non nuls (autrement dit les **résidus quadratiques modulo** p). Soit α un générateur du groupe multiplicatif cyclique $(\mathbb{Z}/p\mathbb{Z})^*$. Ainsi :

$$(\mathbb{Z}/p\mathbb{Z})^* = \{1, \alpha, \alpha^2, \cdots, \alpha^{p-2}\}.$$

Dans un premier temps nous allons montrer que la moitié exactement des éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ sont des résidus quadratiques.

Théorème 1.1 *Soit p un nombre premier impair. Un générateur α de $(\mathbb{Z}/p\mathbb{Z})^*$ n'est pas un résidu quadratique. De plus dans $(\mathbb{Z}/p\mathbb{Z})^*$*

$$\alpha^{\frac{p-1}{2}} = -1.$$

Preuve. On sait d'après le petit théorème de Fermat que $\alpha^{p-1} = 1$. On en déduit que $\alpha^{\frac{p-1}{2}} = \pm 1$. Mais comme α est, par définition, d'ordre $p-1$, on a nécessairement $\alpha^{\frac{p-1}{2}} = -1$. Si α était un carré on aurait $\alpha = \beta^2$ et donc on aurait $\alpha^{\frac{p-1}{2}} = \beta^{p-1} = 1$, ce qui n'est pas. □

Théorème 1.2 *Soit p un nombre premier impair et soit α un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Dans $(\mathbb{Z}/p\mathbb{Z})^*$ les résidus quadratiques sont les puissances paires de α. Ainsi la moitié des $p-1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ sont des résidus quadratiques.*

Preuve. Il est clair qu'une puissance paire α^{2k} de α admet deux racines carrées $\pm\alpha^k$. Si maintenant on prend un nombre de la forme α^{2k+1} il ne peut pas être de la forme u^2. Sinon on aurait $\alpha = \frac{u^2}{\alpha^{2k}}$, c'est-à-dire que α serait un carré, ce qui n'est pas. □

Définition 1.3 *Soit p un nombre premier impair et soit a un entier. Nous définissons le symbole de Legendre de a par :*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \textit{si a est divisible par p} \\ 1 & \textit{si a est un résidu quadratique modulo p} \\ -1 & \textit{si a n'est pas divisible par p et n'est pas un résidu quadratique} \end{cases}$$

Remarque: Le symbole de Legendre de a ne dépend que de la classe de a modulo p :

$$\left(\frac{a}{p}\right) = \left(\frac{a \mod p}{p}\right).$$

Théorème 1.4 *Si a est premier avec p alors :*

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}.$$

Preuve. Soit α un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Quitte à considérer $a \mod p$, on peut écrire a sous la forme $a = \alpha^k$. Donc :

$$a^{\frac{p-1}{2}} = \left(\alpha^{\frac{p-1}{2}}\right)^k = (-1)^k.$$

Le théorème 1.2 permet de conclure. □

Remarque:
1) Le symbole de Legendre est donc directement lié à la notion de résidu quadratique. Le symbole de Legendre de a modulo p vaut 1 si et seulement si a est un résidu quadratique.
2) L'expression du symbole de Legendre donné dans le théorème précédent nous permet de le calculer en temps polynomial, grâce à l'algorithme de calcul de puissance square and multiply.
3) Le symbole de Legendre est multiplicatif :

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

2 Le cas d'un nombre composé

Nous allons nous intéresser maintenant au cas où le module n n'est pas un nombre premier. Dans ce cas nous allons généraliser le symbole de Legendre en définissant le symbole de Jacobi.

Définition 2.1 *Soit n un entier impair ≥ 3 que nous décomposons sous la forme $n = p_1 p_2 \cdots p_s$ où les p_i sont des nombres premiers (non nécessairement distincts). Soit a un entier. Nous définissons le symbole de Jacobi de a modulo n par :*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right).$$

Remarque:
1) Lorsque n est premier impair, le symbole de Jacobi coïncide avec le symbole de Legendre.
2) Le symbole de Jacobi de a ne dépend que de la classe de a :

$$\left(\frac{a}{n}\right) = \left(\frac{a \mod n}{n}\right).$$

3) Le symbole de Jacobi est multiplicatif en ses deux arguments :

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right),$$

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$$

4) Si a n'est pas premier avec n alors :

$$\left(\frac{a}{n}\right) = 0.$$

Si on sait factoriser n, le calcul du symbole de Jacobi passe par le calcul d'un certain nombre de symboles de Legendre. Si n est trop grand pour être factorisé efficacement on peut tout de même calculer le symbole de Jacobi de manière efficace grâce aux deux propositions suivantes.

Théorème 2.2 *Soit $n > 3$ un entier impair. Alors :*

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}},$$

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Théorème 2.3 (Loi de réciprocité quadratique) *Soient m et n des entiers impairs > 3. Alors :*

$$\left(\frac{m}{n}\right) = (-1)^{\frac{(n-1)(m-1)}{4}} \left(\frac{n}{m}\right).$$

Voici un algorithme polynomial qui permet alors de calculer le symbole de Jacobi. On se donne un entier n impair ≥ 3 et un entier m. On se propose de calculer $\left(\frac{m}{n}\right)$.

$N := n$; $M := m$; $S := 1$;
si $M < 0$ **alors**
  $M := -M$;
  $S := (-1)^{\frac{N-1}{2}}$;
finsi
Tant que $M \geq 2$ **faire**
  si M pair **alors**
    $M := M/2$;
    $S := S * (-1)^{\frac{N^2-1}{8}}$;
  sinon
    $S := S * (-1)^{\frac{(N-1)(M-1)}{4}}$;
    $Aux := Reste\_Division(N, M)$;
    $N := M$;
    $M := Aux$;
  finsi
fintq
si $M = 0$ **alors** $S = 0$;

En sortie, S contient le symbole de Jacobi cherché. On laissera au lecteur le soin de vérifier que :

$$\left(\frac{m}{n}\right) = S\left(\frac{M}{N}\right)$$

est un invariant de boucle.

Remarque: Le symbole de Jacobi modulo n ne caractérise pas les résidus quadratiques modulo n. Clairement, si a est un résidu quadratique modulo n, alors son symbole de Jacobi est 1. Mais la réciproque est fausse en général. La situation n'est plus aussi simple que dans le cas d'un module premier (symbole de Legendre). Nous venons de voir, grâce à l'algorithme précédent, que le calcul du symbole de Jacobi d'un entier modulo n est polynomial en la taille de n. En revanche, déterminer si un entier est un résidu quadratique ou non, modulo un produit $n = pq$ de deux nombres premiers p et q, est un problème qu'on ne sait pas résoudre en temps polynomial si on ignore la factorisation de n.

3 Utilisation des résidus quadratiques en cryptographie

On a vu que le problème de déterminer lorsque n est un nombre composé, si un nombre est un résidu quadratique ou pas est difficile. Ce problème est utilisé en cryptographie. Si on sait qu'un nombre est un résidu quadratique, en trouver une racine carrée modulo n (lorsque n est composé) est aussi un problème difficile. Ce dernier problème est aussi utilisé dans divers mécanismes cryptographiques.