Symbole de Legendre

Définition 1 *Le symbole de Legendre* $\left(\frac{a}{p}\right)$ *est défini pour tout* $a \in \mathbb{Z}$ *et* $p \neq 2$, p *premier par*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \mod p, \\ +1 & \text{si } a \text{ est un carré non nul} \mod p, \\ -1 & \text{si } a \text{ n'est pas un carré non nul} \mod p. \end{cases} \quad (1)$$

Si $\left(\frac{a}{p}\right) = +1$ on dit que a est un résidu quadratique. Si $\left(\frac{a}{p}\right) = -1$ on dit que a est un non résidu quadratique.
$a \in \mathbb{Z}_p^*$ est un résidu quadratique si et seulement si c'est un carré dans $\mathbb{Z}_p^*$, c'est-à-dire si et seulement s'il existe $x \in \mathbb{Z}_p^*$ tel que $a = x^2$ dans $\mathbb{Z}_p^*$, ($a \equiv x^2 \mod p$).

Propriété 1

i) Pour $a, b \in \mathbb{Z}$

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

ii) Pour $a \in \mathbb{Z}$

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

iii) Pour tout $p \neq 2$

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

iv) (Loi de réciprocité quadratique) Pour p, q *premiers impairs et distincts*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Symbole de Jacobi Généralisation du symbole de Legendre.

Définition 2 *Le symbole de Jacobi est défini pour* $a \in \mathbb{Z}$ *et* $n > 2$, $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ *impair par*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \dots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

En particulier $\left(\frac{0}{n}\right) = 0$ et $\left(\frac{1}{n}\right) = 1$.

Lemme 2 *Pour* $n, m \in \mathbb{Z}$, *impairs,*

i) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ *et* $\left(\frac{a}{n}\right) = 0$ *si et seulement* $\operatorname{pgcd}(a, n) > 1$.

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

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

Remarque. D'après la définition du symbole de Legendre, pour tout $m = p$ premier impair et tout $a = n \in \mathbb{Z}_p$ non nul, n est un résidu quadratique $\mod m$ si et seulement si $\left(\frac{n}{m}\right) = +1$.
Lorsque $m > 2$ est impair et pas nécessairement premier, on n'a plus d'équivalence, il arrive parfois que n ne soit pas un résidu quadratique $\mod m$ et que pourtant $\left(\frac{n}{m}\right) = +1$.

1) Si n est un résidu quadratique $\mod m$, alors $\left(\frac{n}{m}\right) = +1$,

2) si $\left(\frac{n}{m}\right) = -1$, alors n n'est pas un résidu quadratique $\mod m$.