Eléments de base de réciprocité quadratique

Julien Baglio
MP Lycée Henri IV

21 mai 2005

Théorème 1 *Soit $\mathbb{F}_p$ le corps à p élements (isomorphe à $\mathbb{Z}/p\mathbb{Z}$) avec p premier ; ce corps contient $\frac{p+1}{2}$ carrés.*

Démonstration

Soit $f : x \in (\mathbb{Z}/p\mathbb{Z})^* \longmapsto x^2$ endomorphisme du groupe multiplicatif du corps $\mathbb{F}_p$. On a $\ker f = \{-1; 1\}$. Or on a $|\mathbb{F}_p^*| = |\operatorname{im} f|.|\ker f|$ donc on a $|\operatorname{im} f| = \frac{p-1}{2}$, ce qui signifie que $\mathbb{F}_p^*$ contient $\frac{p-1}{2}$ carrés ; en rajoutant 0 qui est un carré de $\mathbb{F}_p$ on obtient le résultat souhaité.

Théorème 2 (Critère d'Euler) *Soit $x \in \mathbb{F}_p$ non nul. Alors x est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.*

Démonstration

Pour x non nul on a $(x^{\frac{p-1}{2}})^2 = x^{p-1} = 1$ par le théorème de Lagrange donc $x^{\frac{p-1}{2}} \in \ker f = \{1; -1\}$.
Si x est un carré non nul alors $x \in \operatorname{im} f$ qui est un sous-groupe de $\mathbb{F}_p^*$ de cardinal $\frac{p-1}{2}$. D'après la remarque ci-dessus, on a $x^{\frac{p-1}{2}} = 1$. De plus, les $\frac{p-1}{2}$ carrés non nuls sont contenus dans l'ensemble des racines du polynôme $X^{\frac{p-1}{2}} - 1$; F_p étant un corps, ce polynôme a au plus $\frac{p-1}{2}$ racines, qui sont exactement les carrés non nuls de $\mathbb{F}_p$, ce que l'on souhaitait démontrer.

On peut étendre ce critère au résidus n-ièmes : $x^n \equiv a_{[p]}$ est résoluble si et seulement si $a^{\frac{p-1}{q}} \equiv 1_{[p]}$ avec $q = \operatorname{pgcd}(p-1, n)$.
Il y a donc q racines modulo p et donc $1 + \frac{p-1}{q}$ résidus n-ièmes dans $\mathbb{Z}/p\mathbb{Z}$.