Idéaux de Carmichael dans les corps de nombres

La théorie des tests de primalité, autrement dit des critères de composition, est essentielle en cryptographie algébrique. Le test de primalité le plus simple, en rapport avec son efficacité, est issu du petit théorème de Fermat. Étant donné un entier $n \geq 2$, s'il existe $a \in \mathbb{Z}$ tel que l'on ait $a^n \not\equiv a$ mod. n, alors n est composé. Cela étant, il existe une infinité d'entiers n composés tels que pour tout $a \in \mathbb{Z}$, on ait $a^n \equiv a$ mod. n. De tels entiers s'appellent des nombres de Carmichael, nom du mathématicien américain qui est resté célèbre pour leur étude au début du vingtième siècle.

Il y a une dizaine d'années, on a étendu la notion de nombre de Carmichael dans le cadre des anneaux d'entiers des extensions finies de $\mathbb{Q}$ i.e. des corps de nombres. On parle alors d'idéaux de Carmichael dans ces anneaux d'entiers. L'objectif de ce mémoire est d'aborder l'étude de ces idéaux en relation avec le test de primalité de Fermat, en utilisant l'article ci-dessous comme référence.

G. A. Steele, Carmichael numbers in number rings, *J. Number Theory*, **128** (2008), 910-917.

Prérequis :

. Début de la théorie des corps de nombres

. Théorie de Galois

Alain Kraus
Bureau : Tour 15-25 - 425
Adresse email : alain.kraus@imj-prg.fr