Séminaire de théorie des nombres

Le 7 mars 2016 à 14h (PRG)

Le crible algébrique et les accouplements de Weil

Exposé de Razvan Barbulescu
(IMJ-PRG)

Résumé :

Dans un groupe fini commutatif G de cardinal connu où on s'est donné deux éléments $g \in G$ et $h \in \langle g \rangle$, le problème du logarithme discret consiste à calculer le plus petit entiers x tel que $h = g^x$. La difficulté de ce problème dépend du groupe G : il est trivial dans le groupe Z/nZ et requiert un nombre exponentiel d'opérations dans le groupe des points rationnels des courbes elliptiques sur un corps fini. Le cas $G = (\mathbb{F}p^n)^*$ est très important grâce à l'introduction des accouplements de Weil en cryptologie.

Pour calculer des logs discrets dans $\mathbb{F}_{p^n}$ on utilise l'algorithme du crible algébrique, qui a été inventé pour factoriser des entiers et adapté ensuite à notre problème. L'enjeu est alors de choisir bien les deux corps de nombres qui interviennent dans l'algorithme, qui sont tels que $\mathbb{F}_{p^n}$ soit représenté comme corps résiduel commun.

Dans cet exposé nous allons voir comment choisir de tels corps de nombres quand n est composé. Cela a comme conséquence que, pour p^n dans un intervalle etroit, la difficulté du problème augmente avec p ou, dit autrement, les plus difficiles corps finis sont les corps premiers.