Séminaire de théorie des nombres

Le 27 octobre 2014 à 14h (Jussieu)

Utilisation des automorphismes de corps de nombres dans le calcul de logarithmes discrets

Exposé de Razvan Barbaud (IMJ-PRG)

Résumé : Le problème du logarithme discret consisteà résoudre l'équation $g^x = h$ où g et h sont deux éléments d'un groupe. Les deux exemples qui ont la plus grande importance cryptographique sont celui des groupes multiplicatifs des corps finis et celui des courbes elliptiques. Pour les corps finis à p^n éléments avec p premier et n petit, le meilleur algorithme connu est le crible algébrique, qui utilise de manière importante les propriétés des corps de nombres. En 2006, Joux, Lercier, Smart et Vercauteren ont proposé d'accélérer les calculs à l'aide des automorphismes des corps de nombres, mais ils se sont limités à un cas particulier.

Dans cet exposé, nous rappelons le crible algébrique, en mettant l'accent sur sa partie mathématique, en particulier en définissant ce qu'on appelle logarithmes virtuels. Cela va nous permettre de prouver des résultats liés à l'utilisation des automorphismes. Nous finirons par regarder U/U^ℓ comme un espace vectoriel où U est le groupe des unités d'un corps de nombres et ℓ un nombre premier. Cela permet de montrer que certains logarithmes discrets sont nuls et d'avoir une accélération supplémentaire.