Séminaire de théorie des nombres

Le 6 Juin 2011 à 14h (Jussieu)

Aspects algorithmiques des représentations galoisiennes modulaires

Exposé de Peter Bruin
(Université Paris Sud)

Résumé : Soit $\mathbf{F}$ un corps fini, et soit ρ une représentation continue, irréductible et impaire du groupe de Galois absolu de $\mathbf{Q}$ dans $\mathrm{GL}_2(\mathbf{F})$. La conjecture de Serre, qui a été démontrée par Khare, Wintenberger et Kisin, dit que ρ est modulaire, c'est-à-dire qu'il existe une forme modulaire f sur $\mathbf{F}$ dont les coefficients sont liés dans un sens précis aux polynômes caractéristiques des éléments de Frobenius sous ρ. J'expliquerai un algorithme qui calcule ρ de façon explicite en temps polynomial probabiliste par rapport au niveau et au poids de f et au cardinal de $\mathbf{F}$, sous l'hypothèse de Riemann généralisée. Cet algorithme, dû à Couveignes, Edixhoven et collaborateurs, dont l'orateur pour l'extension aux niveaux > 1, utilise des calculs dans les jacobiennes de courbes modulaires sur des corps finis pour 'approcher' ρ. Un autre ingrédient essentiel est une majoration de la précision requise au moyen de la théorie d'Arakelov.