MT 803D - Tópicos em Matemática Aplicada
Geometria dos Números

Data: 21/11/2014 (Sexta-Feira)
Local: Sala 224, IMECC

14h: Criptografia Baseada em Reticulados
Maiara Francine Bollauf - Unicamp

Resumo: Todo sistema criptográfico está baseado em problemas difíceis em Matemática. A estrutura de reticulados, por sua vez, nos traz dois problemas difíceis: problema do vetor mais curto (SVP) e o problema do vetor mais próximo (CVP). Vamos apresentar então esses problemas e estudar dois criptossistemas baseados em chaves públicas que estão fundamentados na dificuldade de resolvê-los, que são o sistema GGH e o NTRU. Acredita-se que tais sistemas criptográficos sejam eficientes na evolução dos computadores clásssicos e ainda, possam resistir à futura implementação do computador quântico.

15h15: Provas alternativas para os Teoremas de Pick e de Ehrhart e Semigrupos Numéricos
Matheus Bernardini de Souza - Unicamp

Resumo: O Teorema de Pick relaciona a quantidade de pontos inteiros em um polígono convexo com a área desse poligono. No final do século XIX, George Pick demonstrou esse resultado e em 2007 Murty e Thain usaram o Teorema de Minkowski para demonstrar o Teorema de Pick.

O Teorema de Ehrhart nos dá uma forma para contagem de pontos inteiros em politopos (inteiros e racionais). Foi originalmente demonstrado na década de 60 por Eugéne Ehrhart e em 2009 Steven Sam deu uma nova demonstração para esse teorema usando o princípio da inclusão-exclusão, como principal ferramenta.

Neste seminário, faremos as ideias usadas nas "novas" demonstrações para os dois teoremas e daremos uma aplicação do Teorema de Ehrhart em Semigrupos Numéricos.