

## **Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos**

Ariane Masuda (University of Ottawa) e  
Daniel Panario (Carleton University)

O objetivo deste curso é apresentar a teoria básica de corpos finitos e mostrar algumas das suas inúmeras aplicações em áreas como Criptografia e Teoria de Códigos. Em particular, as operações aritméticas em corpos finitos exercem um papel fundamental nessas aplicações. Alguns dos algoritmos principais utilizados recentemente na multiplicação e na exponenciação de elementos num corpo finito serão discutidos neste curso. Vários resultados sobre polinômios irredutíveis e elementos normais serão cobertos. A pesquisa na área da teoria de corpos finitos e aplicações tem crescido muito nos últimos anos. Vários problemas em aberto também serão apresentados. O curso é introdutório, e o único pré-requisito é um curso de Álgebra.