DE PRIMA LECTURE

TUESDAY, NOVEMBER 7, 2023 IN 310 LINDE HALL AT 4PM

"THE SEARCH FOR SUPERSINGULAR CURVES"

In this talk, I will explain what it means for a curve over a finite field to be supersingular. I will briefly describe why supersingular curves are useful (or not!) for cryptography. I will describe some open conjectures about whether supersingular curves exist (for arbitrary genus and characteristic), and then some evidence for the conjectures and reasons to think they may be false. At the end, I will discuss some research results (joint with Li, Mantovan, Tang) about the existence of supersingular curves of genus 6 and 7.

RACHEL PRIES
Colorado State University

Getting Here: Parking is available in Lot 3 (underground parking #126 on campus map) on California Blvd. between Wilson and Arden (near the tennis courts). Linde Hall is located directly across the street.

Questions? Please email mathinfor@caltech.edu or call 626-395-4335