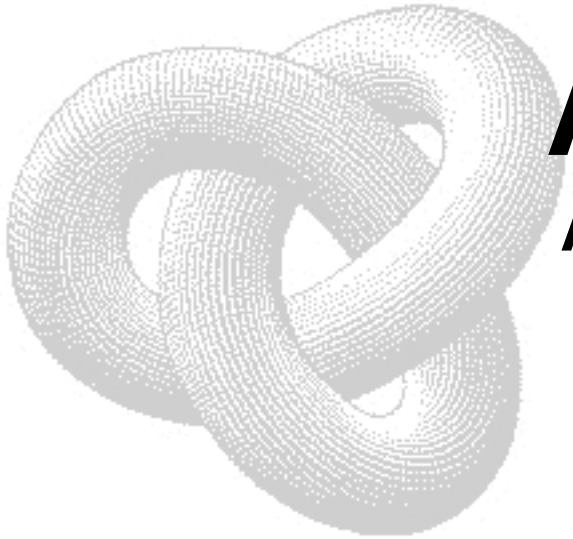
Lectures on Pure and Applied Math

Research Topics in the Mathematical Sciences



Announcing

A Seminar Presentation on March 13, 2014 at 1:45 pm in Lee 301

at The University of New Haven

Dr. Reinier Broker
Department of Mathematics, Brown University

Constructing Elliptic Curves of Prescribed Order

Abstract:

Elliptic curves have become increasingly important during the last 20 years. They play a key role in Wiles' proof of Fermat's last theorem, and they are one of the foundations of modern cryptography: every cell phone contains an elliptic curve nowadays. There are various efficient algorithms to count the number of points of a given elliptic curve over a finite field. In this talk we will consider the inverse problem of constructing elliptic curves of prescribed order. We'll present a solution that easily handles the sizes occurring in cryptographic practice. Many examples will be given.

Further Information

For further information, please contact Carole McClellan at the Department of Mathematics, Office: Maxcy 204, 203-932-7250, CMcClellan@newhaven.edu.