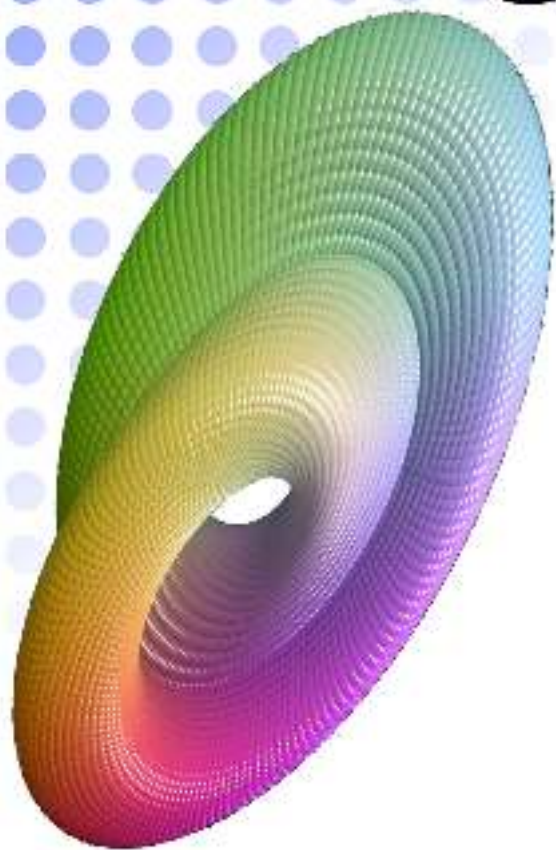# Michigan Math Club

Thursday at 4pm in the Nesbitt Room
Free Pizza and Pop

Using Modular Arithmetic and Elliptic Curves in Cryptography

Valia Gazaki

Abstract for 9 November

In this talk we will introduce two different public-key Cryptography methods, using only basic knowledge of modular arithmetic. First, we will talk about the RSA encryption, whose safety is based on the intractability of factoring large positive integers into products of prime numbers. Second, we will introduce the notion of an elliptic curve, give a geometric description of the addition law on points of such a curve and describe the "Elliptic Curve Cryptography (ECC)".