SE&T Colloquium Series-Fall 2016

Speaker	Mr. Dylan McKnight President of SVSU Math Club Advisor: Dr. Tony Crachiola
Title	*Exploring Elliptic Curves Using Maple*
Abstract	Elliptic curves are a family of equations that have been at the forefront of modern mathematics research. They have been utilized in topics ranging from Integer factoring, Cryptography, to helping prove Fermat's Last Theorem. If we analyze these equations through the lens of basic abstract algebra, many interesting properties come to light. We will explore these topics using Maple. Maple is a ubiquitous CAS (Computer Algebra System) that has a wide variety of uses, from integrating and differentiating, to general programming. Many of the programs, called procedures in Maple, have been written specifically for the purpose of analyzing elliptic curves, and the algorithms will be explored in the course of the talk. Utilizing the "chord and tangent" method of point addition over elliptic curves, the set of solutions to the elliptic curve equation $y^2 = x^3 + ax + b$ forms an abelian group. When the curve is taken over a finite field, such as Z_p, the resulting finite abelian group's structure can be analyzed, and patterns can be found. With Maple, we may construct the finite abelian group, add elements of the group, and construct the addition table for the group. From these addition tables, we can demonstrate properties the group more clearly.
Date	Tuesday, October 18
Time	4:10-5:00pm
Place	Pioneer 240
	Refreshments will be served at 4:00pm.