1035-G1-913

**John H. Wilson*** (john.wilson@centre.edu), Centre College, 600 West Walnut Street,
Danville, KY 40422. *Cyclic Patterns of Points on Koblitz Curves.* Preliminary report.

Koblitz curves are a class of elliptic curves defined over finite fields of characteristic two. The points on any elliptic curve form an abelian group. The security of elliptic curve cryptography, a public key system, is based on the difficulty of solving the discrete logarithm problem in these groups. In this talk, patterns in the doubling orbit of points will be shown. These patterns could be useful in solving the discrete logarithm problem for Koblitz curves. The patterns were discovered by undergraduates while studying Koblitz curves of small order. Several questions for further research will be given. (Received September 17, 2007)