1070-14-282 **Emma Previato** (ep@math.bu.edu), Boston University, Department of Mathematics, 111 Cummington Street, Boston, MA 02215, and **Michael Robertson*** (mrob@bu.edu). *Number of points on elliptic curves over families.*

Adapting, and experimenting with, Schoof's algorithm to count the number of points of an elliptic curve: $y^2 = x^3 + Ax + B$ over a finite field (characteristic $p \neq 2$) of p^k elements, the following observation was made: calling this number $\zeta(A, B)$ (for it is a zeta-function value), we noticed when $p \equiv 1 \pmod 4$, $\zeta(A, B) = \zeta(A, -B)$, whereas when $p \equiv 3 \pmod 4$, $\zeta(A, B) + \zeta(A, -B) = 2(p^k + 1)$, so that, in particular, if one curve has the maximum possible number of points among elliptic curves over that field, the other has the minimum. In this talk, our experiments will be illustrated with tables and a theoretical proof of the observation will be sketched. We are in the process of completing the analysis for $p = 2$, and intend to look for analogous properties in the case of hyperelliptic curves, $y^2 = x^{2g+1} + A_{2g-1}x^{2g-1} + ... + A_0$. This project was funded by UROP (Undergraduate Research Opportunities Program) of Boston University in the summer 2010, with the title "Elliptic Curve Cryptography," under the advisorship of Emma Previato. (Received February 14, 2011)