AIDEN A. BRUEN, University of Calgary, 2500 University Drive NW, Calgary, Alberta, T2G 1N4

Elliptic curves in cryptography and geometry

This lecture describes joint work with James Hirschfeld and David Wehlau. In the lecture I focus on 2 main topics:

(1) A clarification of the actual definition of an elliptic curve, both historically, and as used in ECC, is presented. From this I then show how the scope of ECC can be significantly widened by adopting a more general approach.

(2) The geometry of elliptic curves. In particular, using classical ideas, I show how to construct new configurations in finite planes having desirable algebraic and combinatorial properties.

This generalizes well-known results of A. Zirilli and P. M. Neumann (relating also to work of Voloch and Alderson–Bruen).

Time permitting I will skirmish with the case of infinite fields.