

1086-11-685

Vorropan Chandee (vorrapan@gmail.com), **Chantal David***
(cdavid@mathstat.concordia.ca), **Dimitris Koukoulopoulos** (dimkouk@gmail.com) and
Ethan Smith (ethancsmith@gmail.com). *Elliptic curves with prescribed groups over finite fields.*

Let $G_{m,k} := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ be an abelian group of rank 2 and order $N = mk^2$. When does there exist a finite field \mathbb{F}_p and an elliptic curve E/\mathbb{F}_p such that $E(\mathbb{F}_p) \simeq G_{m,k}$? It was conjectured by Banks, Pappalardi and Shparlinski that this happens with density 0 if the group is “too split”, namely if $k \ll (\log m)^{2-\varepsilon}$, and with density 1 if $k \gg (\log m)^{2+\varepsilon}$. We prove in this talk that the first part of the conjecture holds for the whole range of m and k , and that the second part holds for the limited range $m \leq k^{1/4+\epsilon}$. We also show that G occurs with positive density for a larger range.

This is joint work with F. Chandee, D. Koukoulopoulos and E. Smith. (Received September 11, 2012)