1077-20-1481 **László Babai*** (lbabai@gmail.com), **Robert Beals** and **Ákos Seress**. *Polynomial-time Theory of Matrix Groups.*

Given a list T of $n \times n$ matrices over a finite field, how difficult is it to determine the order of the group G generated by T and to decide membership in G? We describe the first definitive theoretical result in this decades-old quest, started by Babai and Szemerédi in 1984. Hard number theoretic problems such as factoring and discrete log stand in the way of polynomial-time solutions even in the 1×1 case. The recent result says that in a well-defined sense, these are in fact the only obstacles, at least in odd characteristic.

The framework of the algorithms is given by the now popular filtration $G \geq \mathrm{Pker}(G) \geq \mathrm{Rad}(G) \geq \{1\}$ introduced by Babai and Beals in 1997. The algorithms build on major recent progress by C. W. Parker and R. A. Wilson on the statistical analysis of Bray's algorithm for the centralizer of an involution in odd characteristic, and a related paper by Holmes et al. Other ingredients from recent progress in statistical group theory include the recognition of finite simple groups by sampling their element orders (Babai - Kantor - Pálfy - Seress) and an estimate of the frequency of r'-elements in finite simple groups (Babai - Pálfy - Saxl). (Received September 19, 2011)