1077-11-377 **Andrew V. Sutherland*** (drew@math.mit.edu), Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139. *Identifying supersingular elliptic curves.*

Given an elliptic curve E over a field of characteristic p, we wish determine whether E is ordinary or supersingular, and to do so as efficiently as possible. I will review the complexity of several existing algorithms, and then present a new approach based on structural differences between ordinary and supersingular isogeny graphs. This yields a simple algorithm that, given E and a suitable non-residue in $\mathbb{F}_p^2$, determines the supersingularity of E in $O(n^3 \log^2 n)$ time and $O(n)$ space, where $n = O(\log p)$. Both these complexity bounds are significant improvements over existing methods. (Received August 26, 2011)