1016-11-121 **Clayton Petsche*** (clayton@math.uga.edu), Department of Mathematics, The University of Georgia, Athens, GA 30602-7403. *Small Rational Points on Elliptic Curves Over Number Fields.*

Let k be a number field of degree $d = [k : \mathbb{Q}]$, and let E/k be an elliptic curve. Merel used deep facts about the arithmetic of modular curves to prove that there is a universal bound $C(d)$ depending only on d such that $|E(k)_{\mathrm{tor}}| \leq C(d)$. Quantitative refinements of Merel's theorem due to Parent and Oesterlé give explicit bounds $C(d)$ which depend exponentially on d, but it is still unknown whether one can take for $C(d)$ an expression whose growth is polynomial in d. Such a bound–or a proof that no such bound is possible–would be of value, both for its intrinsic interest and for its implications in cryptography. I will give an explicit polynomial bound on $|E(k)_{tor}|$ depending on d and the Szpiro ratio σ, a certain quantity associated to the elliptic curve E/k, which is conjecturally bounded independently of E/k. The same method allows one to obtain polynomial lower bounds on the Néron-Tate height of nontorsion points, also depending on d and σ. (Received February 07, 2006)