1067-11-436 **Andrew V Sutherland*** (drew@math.mit.edu), Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139. *Genus 1 point counting in quadratic space and essentially quartic time.*

The Schoof-Elkies-Atkin (SEA) algorithm is the method of choice for counting points on an elliptic curve modulo a prime p. Its main limitation is the size of the modular polynomials it requires. The largest of these uses on the order of $n^3 \log n$ bits of storage, where $n = \log p$, and their aggregate size is quartic in n.

I will describe a modified version of the SEA algorithm that requires only quadratic space, based on a method for directly computing instantiated modular polynomials via an explicit form of the Chinese remainder theorem. This algorithm is not only able to handle much larger problem sizes, its reduced space complexity also yields a better running time. These results have led to a new point counting record, modulo a prime p with more than 5000 decimal digits. Time permitting, I will discuss how the same techniques may be applied to some other problems in computational number theory. (Received September 03, 2010)