

1125-11-577

**Andrew V Sutherland\*** ([drew@math.mit.edu](mailto:drew@math.mit.edu)), Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Ave., Cambridge, MA 02139. *Computing L-series of genus 3 curves*. Preliminary report.

The efficient computation of L-series of low genus curves raises two closely related algorithmic problems that have applications to cryptography: counting points on curves over finite fields and performing group operations in their Jacobians. These have been extensively studied in genus 1 and 2, but genus 3 raises several new challenges. In particular, one must consider curves that are not hyperelliptic, and even for hyperelliptic curves, many of the algorithms that work well in genus 1 and 2 do not easily generalize to practical algorithms in genus 3.

I will discuss recent progress in both the hyperelliptic and non-hyperelliptic cases. (Received September 06, 2016)