Identifying supersingular elliptic curves

Andrew V. Sutherland

(Submitted on 6 Jul 2011 (v1), last revised 5 Sep 2012 (this version, v3))

Given an elliptic curve E over a field of positive characteristic p, we consider how to efficiently determine whether E is ordinary or supersingular. We analyze the complexity of several existing algorithms and then present a new approach that exploits structural differences between ordinary and supersingular isogeny graphs. This yields a simple algorithm that, given E and a suitable non-residue in 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, as we demonstrate with some practical computations.

Comments:	minor edits, 10 pages, to appear in the LMS Journal of Computation and Mathematics
Subjects:	**Number Theory (math.NT)**
MSC classes:	11G07 (Primary) 11Y16, 11G20, 14H52 (Secondary)
Cite as:	**arXiv:1107.1140 [math.NT]**
	(or **arXiv:1107.1140v3 [math.NT]** for this version)

Submission history

From: Andrew Sutherland [view email]
[v1] Wed, 6 Jul 2011 14:22:37 GMT (14kb)
[v2] Sat, 31 Dec 2011 21:43:13 GMT (14kb)
[v3] Wed, 5 Sep 2012 16:01:45 GMT (14kb)

Which authors of this paper are endorsers?

Download:

- PDF
- PostScript
- Other formats

Current browse context:

math.NT

< prev | next >

new | recent | 1107

Change to browse by:

math

References & Citations

- NASA ADS

Bookmark(what is this?)