Heuristics on pairing-friendly elliptic curves

John Boxall

(Submitted on 1 Jul 2011 (v1), last revised 1 Apr 2012 (this version, v3))

We present a heuristic asymptotic formula as $x\to \infty$ for the number of isogeny classes of pairing-friendly elliptic curves with fixed embedding degree $k\geq 3$, with fixed discriminant, with rho-value bounded by a fixed ρ_0 such that $1<\rho_0<2$, and with prime subgroup order at most x.

Comments:	text substantially rewritten, tables corrected
Subjects:	**Number Theory (math.NT)**
MSC classes:	11N56, 11N25, 11T71, 14H52
Cite as:	**arXiv:1107.0307 [math.NT]**
	(or **arXiv:1107.0307v3 [math.NT]** for this version)

Submission history

From: John Boxall [view email]
[v1] Fri, 1 Jul 2011 19:22:07 GMT (17kb)
[v2] Tue, 12 Jul 2011 16:21:05 GMT (20kb)
[v3] Sun, 1 Apr 2012 15:22:03 GMT (20kb)

Which authors of this paper are endorsers?

Link back to: arXiv, form interface, contact.

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?)