zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Bröker, Reinier; **Howe, Everett W.**; **Lauter, Kristin E.**; **Stevenhagen, Peter**

Genus-2 curves and Jacobians with a given number of points. (English) Zbl 1387.14086

LMS J. Comput. Math. 18, 170-197 (2015).

Given an algebraic variety V over a finite field $\mathbb{F}_q$, there are only finitely many rational points on V as V is of finite type. So it becomes a problem of counting the number of rational points for such varieties. The paper under review considers the converse of this problem:

Given a positive integer N, how to construct a finite field $\mathbb{F}_q$ and smooth varieties V such that the set of rational points $V(\mathbb{F}_q)$ has cardinality N.

In [Math. Comput. 76, No. 260, 2161–2179 (2007; Zbl 1127.14022)], *R. Bröker* and *P. Stevenhagen* deal with the problem for elliptic curves. In this paper the authors generalize the result of [loc. cit.] to curves of genus 2.

For a smooth projective connected curve C over a field k, one can define an abelian variety $J(C)$ which is isomorphic to $\mathrm{Pic}^0_{C/k}$. Choosing a point in $C(k)$, one can imbed C into $J(C)$, and this imbedding is an isomorphism if C is an elliptic curve. This leads to two generalizations of the problem to genus 2 case:

- Construct a finite field $\mathbb{F}_q$ and curves of genus 2 with N $\mathbb{F}_q$-rational points;
- Construct a finite field $\mathbb{F}_q$ and curves of genus 2 whose Jacobian has N $\mathbb{F}_q$-rational points;

In this paper the authors consider both of the generalisations.

Reviewer: Lei Zhang (Berlin)

Cited in **1** Review
Cited in **6** Documents

MSC:

14H45 Special algebraic curves and curves of low genus
14K22 Complex multiplication and abelian varieties
11G15 Complex multiplication and moduli of abelian varieties
11G20 Curves over finite and local fields
14G15 Finite ground fields in algebraic geometry
14H40 Jacobians, Prym varieties

Keywords:

genus; curves; Jacobian

Full Text: DOI arXiv

References:

[1] DOI: 10.1515/form.2004.013 · Zbl 1098.14017 · doi:10.1515/form.2004.013
[2] DOI: 10.1515/form.2000.008 · Zbl 0983.11037 · doi:10.1515/form.2000.008
[3] DOI: 10.1007/978-1-4612-0441-1_21 · doi:10.1007/978-1-4612-0441-1_21
[4] DOI: 10.1093/qmath/ham021 · Zbl 1141.11042 · doi:10.1093/qmath/ham021
[5] DOI: 10.4064/aa121-3-1 · Zbl 1122.11053 · doi:10.4064/aa121-3-1
[6] Legendre, Traité des fonctions elliptiques et des intégrales Eulériennes, Tome troisième (1828)
[7] Hermite, Ann. Soc. Sci. Bruxelles Sér. I 1, 2nd part pp 1– (1876)
[8] Kuhn, Trans. Amer. Math. Soc. 307 pp 41– (1988)
[9] Goursat, Bull. Soc. Math. France 13 pp 143– (1885) · Zbl 17.0466.01 · doi:10.24033/bsmf.300
[10] DOI: 10.1007/978-1-4612-0457-2_7 · doi:10.1007/978-1-4612-0457-2_7
[11] Kani, J. reine angew. Math. 485 pp 93– (1997)
[12] DOI: 10.1007/3-540-45455-1_23 · doi:10.1007/3-540-45455-1_23
[13] Jacobi, Gesammelte Werke, Bände I–VIII (1969)
[14] Jacobi, J. reine angew. Math. 8 pp 413– (1832)

Edited by FIZ Karlsruhe, the European Mathematical Society and the Heidelberg Academy of Sciences and Humanities
© 2021 FIZ Karlsruhe GmbH

[15] Eisenträger, Arithmetics, geometry and coding theory (AGCT 2005) 21 pp 161– (2010)

[16] DOI: 10.5802/aif.2430 · Zbl 1236.11058 · doi:10.5802/aif.2430

[17] DOI: 10.1023/A:1016310902973 · Zbl 1050.11104 · doi:10.1023/A:1016310902973

[18] DOI: 10.1090/S0025-5718-07-01980-1 · Zbl 1127.14022 · doi:10.1090/S0025-5718-07-01980-1

[19] Bröker, J. Comb. Number Theory 1 pp 269– (2009)

[20] DOI: 10.1112/plms/83.3.532 · Zbl 1016.11037 · doi:10.1112/plms/83.3.532

[21] DOI: 10.1007/BFb0058807 · doi:10.1007/BFb0058807

[22] DOI: 10.1112/S1461157012001015 · Zbl 1343.11098 · doi:10.1112/S1461157012001015

[23] DOI: 10.1090/S0025-5718-2013-02712-3 · Zbl 1322.11066 · doi:10.1090/S0025-5718-2013-02712-3

[24] DOI: 10.1007/978-1-4613-8655-1_7 · doi:10.1007/978-1-4613-8655-1_7

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.