Adleman, Leonard M.; **Huang, Ming-Deh A.**

Counting rational points on curves and abelian varieties over finite fields. (English)

Zbl 0898.11045

Cohen, Henri (ed.), Algorithmic number theory. Second international symposium, ANTS-II, Talence, France, May 18-23, 1996. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1122, 1-16 (1996).

Let A be an abelian variety of dimension g over a finite field $\mathbb{F}_q$. Suppose that A is given as a closed subvariety of projective n-space. The authors exhibit a deterministic algorithm that computes the characteristic polynomial of the Frobenius endomorphism of A that runs in time $O((\log q)^c)$, where c is a polynomial expression in g as well as n. This improves upon an earlier result of *J. Pila* [Math. Comput. 55, 745-763 (1990; Zbl 0724.11070)], who obtained a similar result but with the constant c depending exponentially on n.

By applying this to the Jacobian varieties of curves X over $\mathbb{F}_q$, one obtains a deterministic algorithm to count the number of $\mathbb{F}_q$-rational points of X that runs in time $O((\log q)^c)$, where c is a polynomial expression in n, as well as the genus g of X. In the special case of hyperelliptic curves of genus g, the authors show that the number of $\mathbb{F}_q$-rational points on X can be counted deterministically in time $(\log q)^{O(g^6)}$. This case is of interest in view of the primality test decribed by the authors in their monograph [Primality testing and abelian varieties over finite fields, Lect. Notes Math. 1512 (Springer-Verlag, 1992; Zbl 0744.11065)].

For the entire collection see [Zbl 0852.00023].

Reviewer: René Schoof (Amsterdam)

MSC:

11Y16	Number-theoretic algorithms; complexity
11G25	Varieties over finite and local fields
11G20	Curves over finite and local fields
14K15	Arithmetic ground fields for abelian varieties
14G05	Rational points
14G15	Finite ground fields in algebraic geometry
14Q05	Computational aspects of algebraic curves
14Q15	Computational aspects of higher-dimensional varieties
14H25	Arithmetic ground fields for curves

Keywords:

abelian variety over a finite field; deterministic algorithm; characteristic polynomial of the Frobenius endomorphism; Jacobian varieties; rational points; hyperelliptic curves; primality test; complexity analysis