zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Pila, J.

**Frobenius maps of abelian varieties and finding roots of unity in finite fields.** (English)
Zbl 0724.11070
Math. Comput. 55, No. 192, 745-763 (1990).

Author's abstract: "We give a generalization to Abelian varieties over finite fields of the algorithm of Schoof for elliptic curves. Schoof showed that for an elliptic curve E over $\mathbb{F}_q$, given by a Weierstrass equation, one can compute the number of $\mathbb{F}_q$- rational points of E in time $O((\log q)^9)$. Our result is the following. Let A be an Abelian variety over $\mathbb{F}_q$. Then one can compute the characteristic polynomial of the Frobenius endomorphism of A in time $O((\log q)^{\Delta})$, where $\Delta$ and the implied constant depend only on the dimension of the embedding space of A, the number of equations defining A and the addition law, and their degrees. The method, generalizing that of Schoof, is to use the machinery developed by Weil to prove the Riemann hypothesis for Abelian varieties. By means of this theory, the calculation is reduced to ideal-theoretic computations in a ring of polynomials in several variables over $\mathbb{F}_q$. As applications we show how to count the rational points on the reductions modulo primes p of a fixed curve over $\mathbb{Q}$ in time polynomial in log p: we show also that, for a fixed prime $\ell$, we can compute the $\ell th$ roots of unity mod p, when they exist, in polynomial time in log p. This generalizes Schoof's application of his algorithm to find square roots of a fixed integer x mod p."

Reviewer: R.Schoof (Povo)

**MSC:**

| | |
|---|---|
| 11Y16 | Number-theoretic algorithms; complexity |
| 14G15 | Finite ground fields in algebraic geometry |
| 68Q25 | Analysis of algorithms and problem complexity |
| 11G15 | Complex multiplication and moduli of abelian varieties |
| 11G25 | Varieties over finite and local fields |
| 14K22 | Complex multiplication and abelian varieties |

Cited in **4** Reviews
Cited in **40** Documents

**Keywords:**

Abelian varieties over finite fields; algorithm of Schoof; rational points; Frobenius endomorphism; roots of unity mod p; polynomial time

**Full Text:** DOI