

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

**Counting points on curves and Abelian varieties over finite fields.** (English) Zbl 0986.11039  
*J. Symb. Comput.* 32, No. 3, 171-189 (2001).

The authors develop efficient methods for deterministic computations with semi-algebraic sets and apply them to the problem of counting points on curves and Abelian varieties over finite fields.

This type of problem has drawn considerable interest in recent years. *R. Schoof* [*Math. Comput.* 44, 483-494 (1985; [Zbl 0579.14025](#))] gave a deterministic polynomial time algorithm for the case of elliptic curves and applied it to solve, for a fixed integer  $a$ ,  $x^2 \equiv a \pmod{p}$  in deterministic polynomial time on input primes  $p$ . *L. M. Adleman* and *M.-D. Huang* [Primality testing and Abelian varieties over finite fields, *Lect. Notes Math.* 1512, Springer-Verlag (1992; [Zbl 0744.11065](#))] proved a primality testing algorithm which involved a random polynomial time algorithm for counting rational points on Jacobians of curves of genus 2 over finite fields. *J. Pila* [*Math. Comput.* 55, 745-763 (1990; [Zbl 0724.11070](#))] showed that for a fixed curve over the rationals, the number of rational points on the reduction of the curve and its Jacobian modulo a prime can be computed in deterministic polynomial time. The result is applied to solve, for fixed  $l$ ,  $\Phi_l(x) \equiv 0 \pmod{p}$  in deterministic polynomial time on input primes  $p$ , where  $\Phi_l$  denotes the  $l$ -th cyclotomic polynomial.

For Abelian varieties, the authors improve on the result of Pila showing that an Abelian variety of dimension  $g$  in  $\mathbb{P}_{\mathbb{F}_q}^N$ , the problem can be solved in  $O(\log q)^\delta$  time, where  $\delta$  is a polynomial in  $g$  and in  $N$ . For Jacobians of hyperelliptic curves, they show an even better result. The number of rational points can be obtained in  $(\log q)^{O(g^2 \log g)}$  time.

Reviewer: [Amílcar Pacheco](#) (Rio de Janeiro)

**MSC:**

[11G20](#) Curves over finite and local fields  
[14G05](#) Rational points  
[11G05](#) Elliptic curves over global fields

Cited in **1** Review  
Cited in **10** Documents

**Keywords:**

[Abelian varieties; curves over finite fields](#)

**Full Text:** [DOI](#)

**References:**

- [1] Adleman, L.M.; Huang, M.-D., Primality testing and abelian varieties over finite fields, (1992), Springer-Verlag Berlin · [Zbl 0744.11065](#)
- [2] Adleman, L.M.; Huang, M.-D., Counting rational points on curves and abelian varieties over finite fields, Proceedings of the 2nd algorithmic number theory symposium (ANTS II), talence, France, (1996) · [Zbl 0898.11045](#)
- [3] Canny, J., Some algebraic and geometric problems in PSPACE, Proceedings of the 20th ACM symposium on the theory of computing, Chicago, U.S.A., (1988), ACM Press New York
- [4] Cantor, D., Computing in the Jacobian of a hyperelliptic curve, *Math. comput.*, V. 48, 95-101, (1987) · [Zbl 0613.14022](#)
- [5] Chow, W.L., On the defining field of a divisor in an algebraic variety, *Am. J. math.*, 72, 247-283, (1950)
- [6] Chow, W.L., The jacobian variety of an abelian variety, *Am. J. math.*, 76, 454-476, (1954)
- [7] Chow, W.L.; van der Warden, B.L., Zur algebraischen geometrie, IX, über zugeordnete formen und algebraische systeme von algebraischen mannigfaltigkeiten, *Math. annalen*, 113, 692-704, (1937) · [Zbl 0016.04004](#)
- [8] Hartshorne, R., Algebraic geometry, (1977), Springer-Verlag · [Zbl 0367.14001](#)
- [9] Huang, M.-D.; Ierardi, D., \textit{counting points on curves over finite fields.} Proceedings of the 32nd IEEE symposium on the foundations of computer science, Palo Alto, (1993)
- [10] D. Ierardi, 1989a
- [11] Ierardi, D., Quantifier elimination in the theory of an algebraically closed field, Proceedings of the 21st ACM symposium on theory of computing, Seattle, U.S.A., (1989), ACM Press New York

- [12] Ierardi, D.; Kozen, D., Parallel resultant computation, Synthesis of parallel algorithms, (1991), Morgan Kaufman
- [13] Mumford, D., Tata lectures on theta II, (1984), Birkhäuser Boston
- [14] Pila, J., Frobenius maps of abelian varieties and finding roots of unity in finite fields, Math. comput., 55, 745-763, (1990) · [Zbl 0724.11070](#)
- [15] Poonen, B., Computational aspects of curves of genus at least 2, Proceedings of the 2nd algorithmic number theory symposium (ANTS II), talence, France, (1996) · [Zbl 0891.11037](#)
- [16] Schoof, R., Elliptic curves over finite fields and the computation of square roots mod P, Math. comput., 44, 483-494, (1985) · [Zbl 0579.14025](#)

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.