AWS 2026: Counting points on hyperelliptic curves over finite fields

David Harvey

1 Overview

The aim of this course is to study algorithms for computing zeta functions of hyperelliptic curves. I will focus in particular on a number of algorithms inspired by my paper [Har15]. These algorithms are p-adic in nature, but are elementary in the sense that they do not involve any cohomology. You can think of this course as a gentle introduction to [Har15], illustrating the main ideas in the simplified context of hyperelliptic curves over prime fields (the paper actually works in a much more general setting).

The course will follow quite closely a previous course I gave on this topic at PCMI 2022. The lecture notes from that course are available at [Har22].

Pre-reading. I recommend taking a look at Section 1 and Section 2 ("A crash course on fast arithmetic") of [Har22] before AWS. Section 2 will be covered to some extent in the PAWS program.

2 Lectures

Approximate lecture schedule:

- Lecture 1 $\approx$ section 3 from the notes.

  Models of hyperelliptic curves. Definition of the zeta function. Weil conjectures.

- Lecture 2 $\approx$ section 4.

  The Hasse–Witt matrix, and the trace formula for counting points modulo p. Computing $L(T) \pmod p$ via naive expansion.

- Lecture 3 $\approx$ section 5 + start section 6.

  Recurrences for coefficients of polynomial powers. Divisions by p, magical bounds on precision loss. Computing $L(T) \pmod p$ via recurrences. Strassen's $p^{1/2}$ algorithm.

- Lecture 4 $\approx$ finish section 6 + section 7.

  Computing $L(T) \pmod p$ in square root time. Accumulating remainder trees. Computing $L(T) \pmod p$ in average polynomial time.

3 Projects

1. The main project will involve developing algorithms for computing $L(T)$ modulo higher powers of p. The starting point is the trace formula from section 8 of the notes, which we will probably not get to during the lectures. Examples of the kinds of algorithms I have in mind can be found among the problems in [Har22, §8.5].

2. A possible side project would be to develop improved algorithms for computing the Wilson remainders $w_p := (p-1)! \pmod{p^2}$, by using the "factorial sieving" idea from [CDP97]. See for example Problems 6.1.8 and 7.1.17 in [Har22]. This has nothing to do with point counting directly, but does involve the various recurrence-solving techniques discussed in the course.

References

[CDP97] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), no. 217, 433–449. MR 1372002 (97c:11004)

[Har15] D. Harvey, *Computing zeta functions of arithmetic schemes*, Proc. Lond. Math. Soc. (3) **111** (2015), no. 6, 1379–1401. MR 3447797

[Har22] ———, *Counting points on hyperelliptic curves over finite fields*, to appear in PCMI proceedings, available at `https://web.maths.unsw.edu.au/~davidharvey/research/pcmi-draft.pdf`, 2022.