Michigan Math. J. 63 (2014), 503–534

Points on Curves in Small Boxes and Applications

Mei-Chu Chang, Javier Cilleruelo,
Moubariz Z. Garaev, José Hernández,
Igor E. Shparlinski, & Ana Zumalacárregui

Abstract. We introduce several new methods to obtain upper bounds on the number of solutions of the congruences

$$f(x) \equiv y \pmod{p} \quad \text{and} \quad f(x) \equiv y^2 \pmod{p},$$

with a prime p and a polynomial f, where (x, y) belongs to an arbitrary square with side length M. We give two applications of these results to counting hyperelliptic curves in isomorphism classes modulo p and to the diameter of partial trajectories of a polynomial dynamical system modulo p.

1. Introduction

1.1. Motivation

Studying the distribution of integer and rational points on curves and, more generally, on algebraic varieties that belong to a given box is a classical topic in analytic number theory. For the case of plane curves with integer coefficients, essentially the best possible results are due to Bombieri and Pila [6; 32; 33]. Furthermore, recently remarkable progress has been made in the case of hypersurfaces and varieties over the rationals; see the surveys [8; 21; 36] and the original works [27; 28; 34].

Significantly less is known about the distribution of points in boxes on curves and varieties in finite fields. For reasonably large boxes, bounds on exponential sums, which are based on deep methods of algebraic geometry, lead to asymptotic formulas for the number of such points; see [17; 18; 26]. Certainly, when the size of the box is decreasing, beyond a certain threshold no asymptotic formula is possible (in fact, the expected number of points can be less than 1). In particular, for such a small box, we can only expect to derive upper bounds on the number of points on curves that hit it. This question has recently been introduced in [13], where a series of general results has been obtained (we also mention the works [9; 12; 42], where this question has been studied for some very special curves).

In this paper, we introduce new ideas and make significant advances in this direction. We find connections between the problem of distribution of points in small boxes on modular curves with some delicate combinations of results from geometry of numbers, Diophantine approximation theory, the Vinogradov mean value theorem, and the Weyl method.

Received May 2, 2013. Revision received April 4, 2014.