Journal of Number Theory 140 (2014) 277–298

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the distribution of the number of points on a family of curves over finite fields

Kit-Ho Mak [a,*], Alexandru Zaharescu [b,1]

[a] *School of Mathematics, Georgia Institute of Technology, 686 Cherry Street, Atlanta, GA 30332-0160, USA*

[b] *Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, IL 61801, USA*

ARTICLE INFO

Article history:
Received 20 June 2013
Received in revised form 29 January 2014
Accepted 31 January 2014
Available online 5 March 2014
Communicated by David Goss

MSC:
11G20
11T55

Keywords:
Rational points
Algebraic curves
Uniform distribution
Congruences

ABSTRACT

Let p be a large prime, $\ell \geqslant 2$ be a positive integer, $m \geqslant 2$ be an integer relatively prime to ℓ and $P(x) \in \mathbb{F}_p[x]$ be a polynomial which is not a complete ℓ'-th power for any ℓ' for which $GCD(\ell', \ell) = 1$. Let $\mathcal{C}$ be the curve defined by the equation $y^\ell = P(x)$, and take the points on $\mathcal{C}$ to lie in the rectangle $[0, p-1]^2$. In this paper, we study the distribution of the number of points on $\mathcal{C}$ inside small rectangles among residue classes modulo m when we move the rectangle around in $[0, p-1]^2$.

1. Introduction

Since Weil's proof of the Riemann hypothesis for algebraic curves over finite fields [31], there have been numerous studies on the number of rational points of an algebraic

* Corresponding author.
E-mail addresses: kmak6@math.gatech.edu (K.-H. Mak), zaharesc@math.uiuc.edu (A. Zaharescu).

[1] The second author is supported by NSF grant number DMS-0901621.

http://dx.doi.org/10.1016/j.jnt.2014.01.012
0022-314X/

curve over a finite field in a specified set of number theoretic interest. Examples include studies of bounds on the number of rational points in a smaller region inside $[0, p-1]^2$ (see for example Myerson [18], Fujiwara [9], Shparlinski and Skorobogatov [27], Skorobogatov [28], Luo [13] and the authors [16]), bounds on the number of points in sets with prescribed congruence conditions on the coordinates (known as Lehmer problems, see for example Zhang [34,35], Cobeli and one of the authors [6], Bourgain, Cochrane, Paulhus and Pinner [2], and the authors [17]), bounds on the number of visible points (see Shparlinski [24], Shparlinski and Voloch [25], Shparlinski and Winterhof [26], Chan and Shparlinski [5], and the authors [17]) and the fluctuations of the number of points among some families of curves (see Kurlberg and Rudnick [11], Xiong [32] and Bucur, David, Feigon, Lalín [3,4]). Bounds for the number of rational points on curves in a small rectangle is crucial in the study of local spacings between fractional parts of $n^2\alpha$, see Rudnick, Sarnak and one of the authors [21,33]. Such questions have applications in mathematical physics, see the works by Berry and Tabor [1], Rudnick and Sarnak [20] and Sarnak [22].

All the above works study analytic aspects of the number of points of families of curves over finite fields, such as bounds on the number of points and the fluctuation of the number of points along a family. In this paper we initiate a new direction of study, namely the study of arithmetic properties of the number of points on curves. As a starting point, in this paper we will focus on curves of the form

$$y^\ell = P(x) \tag{1.1}$$

over $\mathbb{F}_p$, when the curve is absolutely irreducible. To make it precise, we take the rational points on the curve $\mathcal{C}$ as a subset in $[0, p-1]^2$, and let $\Omega \subseteq [0, p-1]^2$ be a rectangular "window". Instead of asking how many points are captured by Ω, we ask the following question: if we move the window around the domain, what is the probability that the number of captured points is even (or odd)? This kind of problem dates back to Gauss when he proved the well-known Gauss lemma for quadratic residues, i.e. if $GCD(a, p) = 1$, then if r is the number of elements in the set $\{a, 2a, \ldots, (\frac{p-1}{2})a\}$ that have least positive residue greater than $p/2$, then the Legendre symbol satisfies $\frac{a}{p} = (-1)^r$. Formulating in our language, this is to consider the number of points on the line $y = ax$ inside the rectangle $[1, (p-1)/2] \times (p/2, p-1]$, and then look at its residue class modulo 2. We also note that the uniformity modulo m of the values of some multiplicative functions, such as the Ramanujan tau function, was investigated by Serre [23]. For more results on the uniform distribution of the values of multiplicative functions modulo m, the reader is referred to the monograph of Narkiewicz [19]. Recently, Lamzouri and one of the authors [12] have studied the distribution of real character sums modulo m.

In the present paper, we ask about the distribution of the number of points captured by the window Ω among each congruence class of m when we move it around the domain. Since it is believed that the set of rational points on a curve exhibits a strong random behavior, one may expect that the above mentioned probability is $1/m$. We prove that