Journal of Number Theory 177 (2017) 528–561

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Distribution of points on cyclic curves over finite fields

Patrick Meisner

Tel Aviv University, Israel

A R T I C L E   I N F O

Article history:
Received 6 September 2016
Received in revised form 19 January 2017
Accepted 20 January 2017
Available online 7 March 2017
Communicated by D. Goss

Keywords:
Curves
Finite fields
Number of points
Cyclic extensions

A B S T R A C T

We determine in this paper the distribution of the number of points on the cyclic covers of $\mathbb{P}^1(\mathbb{F}_q)$ with affine models $C : Y^r = F(X)$, where $F(X) \in \mathbb{F}_q[X]$ and rth-power free when q is fixed and the genus, g, tends to infinity. This generalizes the work of Kurlberg and Rudnick and Bucur, David, Feigon and Lalin who considered different families of curves over $\mathbb{F}_q$. In all cases, the distribution is given by a sum of random variables.

1. Introduction

Let C be a smooth projective curve over $\mathbb{F}_q$. We will use the notation $\#C(\mathbb{P}^1(\mathbb{F}_q))$ to mean the number of projective points on C and $\#C(\mathbb{F}_q)$ to mean the number of affine points on C. If C has genus g then by the Weil conjectures (see Theorem 5.12 of [8]) we know that

$$\#C(\mathbb{P}^1(\mathbb{F}_q)) = q + 1 - \sum_{j=1}^{2g} \alpha_j(C), \tag{1.1}$$

E-mail address: meisner@mail.tau.ac.il.

http://dx.doi.org/10.1016/j.jnt.2017.01.013

where the zeta function of C is

$$Z_C(u) = \frac{\prod_{j=1}^{2g}(1-u\alpha_j(C))}{(1-q)(1-qu)},$$

where $u = q^{-s}$ and $|\alpha_j(C)| = q^{\frac{1}{2}}$ for $j = 1, \ldots, 2g$.

The distribution of $\#C(\mathbb{P}^1(\mathbb{F}_q))$ when C varies over families of curves over $\mathbb{F}_q$ is a classical object of study. For several families of curves over $\mathbb{F}_q$ Katz and Sarnak [5] showed that when the genus is fixed and q tends to infinity

$$\frac{\sum_{j=1}^{2g}\alpha_j(C)}{\sqrt{q}}$$

is distributed as the trace of a random matrix in the monodromy group of the family.

The distribution of the number points on families of curves over finite fields with q fixed while the genus tends to infinity has been a topic of much research recently. It began with Kurlberg and Rudnick [6] determining the distribution of the number of points of hyperelliptic curves. Hyperelliptic curves are in one-to-one correspondence with Galois extensions of $\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/2\mathbb{Z}$. Bucur, David, Feigon and Lalin [3,2] extended this result to the irreducible moduli space of smooth projective curves that are in one-to-one correspondence with Galois extensions of $\mathbb{F}_q(X)$ with Galois group $\mathbb{Z}/p\mathbb{Z}$, where p is a prime such that $q \equiv 1 \mod p$. Bucur et al. [1] further extended this to the whole moduli space whereas Cheong, Matchett-Wood and Zaman [4] considered the case of superelliptic curves. Recently Lorenzo, Meleleo, Milione and Bucur [7] determined the case for n-quadratic curve (Galois group $(\mathbb{Z}/2\mathbb{Z})^n$). In this paper we determine the case for the irreducible moduli space of curves with cyclic Galois groups $\mathbb{Z}/r\mathbb{Z}$ for any $q \equiv 1 \mod r$ where r is not necessarily a prime.

Let $K = \mathbb{F}_q(X)$ and let L be a finite Galois extension of K. Let r be an integer such that $q \equiv 1 \mod r$. Suppose that $\mathrm{Gal}(L/K) = \mathbb{Z}/r\mathbb{Z}$. Then there exists a unique smooth projective curve over $\mathbb{F}_q$, C, such that $L \cong K(C)$. Further, C will have an affine model of the form

$$Y^r = \alpha F(X), \qquad F \in \mathcal{F}_{(d_1,\ldots,d_{r-1})} \subset \mathbb{F}_q[X], \alpha \in \mathbb{F}_q^*$$

where

$$\mathcal{F}_{(d_1,\ldots,d_{r-1})} = \{F = f_1 f_2^2 \cdots f_{r-1}^{r-1} : f_i \in \mathbb{F}_q[X] \text{ are monic, square-free, pairwise coprime,}$$
$$\text{and } \deg f_i = d_i \text{ for } 1 \leq i \leq r-1\}.$$

The Riemann–Hurwitz formula (Theorem 7.16 of [8]) tells us that if we let $d = \sum_{i=1}^{r-1} i d_i$, then the genus g of the curve C is given by

$$2g + 2r - 2 = \sum_{i=1}^{r-1}(r-(r,i))d_i + (r-(r,d)), \tag{1.2}$$