Journal of Number Theory 156 (2015) 414–431

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Decomposing Jacobians of curves over finite fields in the absence of algebraic structure

Omran Ahmadi [a,*,1], Gary McGuire [b,2], Antonio Rojas-León [c,3]

[a] School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran
[b] School of Mathematical Sciences, University College, Dublin, Ireland
[c] Department of Algebra, University of Seville, Spain

A R T I C L E   I N F O

Article history:
Received 17 November 2014
Accepted 18 April 2015
Available online 9 June 2015
Communicated by D. Wan

MSC:
14H45
11M38

Keywords:
Curve
Jacobian
Supersingular
Finite field
L-polynomial

A B S T R A C T

We consider the issue of when the L-polynomial of one curve over $\mathbb{F}_q$ divides the L-polynomial of another curve. We prove a theorem which shows that divisibility follows from a hypothesis that two curves have the same number of points over infinitely many extensions of a certain type, and one other assumption. We also present an application to a family of curves arising from a conjecture about exponential sums. We make our own conjecture about L-polynomials, and prove that this is equivalent to the exponential sums conjecture.

* Corresponding author.
E-mail addresses: oahmadid@ipm.ir (O. Ahmadi), gary.mcguire@ucd.ie (G. McGuire), arojas@us.es (A. Rojas-León).

[1] Research supported by IPM.
[2] Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.
[3] Partially supported by MTM2010-19298 (Min. Ciencia e Innovación) and FEDER.

http://dx.doi.org/10.1016/j.jnt.2015.04.014
0022-314X/

1. Introduction

Let $q = p^a$ where p is a prime, and let $\mathbb{F}_q$ denote the finite field with q elements. Let $C = C(\mathbb{F}_q)$ be a projective smooth absolutely irreducible curve of genus g defined over $\mathbb{F}_q$. For any $n \geq 1$ let $C(\mathbb{F}_{q^n}) = C(\mathbb{F}_q) \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ be the set of $\mathbb{F}_{q^n}$-rational points of C, and let $\#C(\mathbb{F}_{q^n})$ be the cardinality of $C(\mathbb{F}_{q^n})$. Similarly, if $\overline{\mathbb{F}_q}$ denotes a fixed algebraic closure of $\mathbb{F}_q$, let $C(\overline{\mathbb{F}_q}) = C(\mathbb{F}_q) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$.

The divisor group of C is the free abelian group generated by the points of $C(\overline{\mathbb{F}_q})$. Thus, a divisor is a formal sum $\sum n_P P$ over all $P \in C(\overline{\mathbb{F}_q})$, where all but finitely many n_P are 0. The degree of a divisor is $\sum n_P$. The divisor of a function in the function field $\overline{\mathbb{F}_q}(C)$ must have degree 0, and is called a principal divisor. The quotient of the subgroup of degree 0 divisors by the principal divisors is denoted $Pic^0(C(\overline{\mathbb{F}_q}))$, and is canonically isomorphic to the Jacobian of C, $Jac(C)(\overline{\mathbb{F}_q})$, after a point at infinity is chosen. The Galois group $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ acts on divisors and divisor classes, and we define $Jac(C) = Jac(C)(\mathbb{F}_q) = Pic^0(C) = Pic^0(C(\mathbb{F}_q))$ to be the divisor classes that are fixed by every element of $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. The Jacobian $Jac(C)$ is an abelian variety of dimension g defined over $\mathbb{F}_q$.

The Frobenius map $\pi : x \mapsto x^q$ on $\overline{\mathbb{F}_q}$ induces a Frobenius map on $C(\overline{\mathbb{F}_q})$. The elements of $C(\mathbb{F}_{q^n})$ are the fixed points of π^n. The Frobenius morphism π induces a map on divisor classes, and hence on the Jacobian, and hence a Frobenius endomorphism on the ℓ-adic Tate module $V_\ell(Jac(C))$. Let $P_C(t)$ denote the characteristic polynomial of the Frobenius endomorphism, which is known to have integer coefficients. An abelian variety defined over $\mathbb{F}_q$ is called $\mathbb{F}_q$-simple if it is not isogenous over $\mathbb{F}_q$ to a product of abelian varieties of lower dimensions. An abelian variety is absolutely simple if it is $\overline{\mathbb{F}_q}$-simple. If $Jac(C)$ is $\mathbb{F}_q$-simple then it can be shown that $P_C(X) = h(X)^e$ where $h(X) \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Z}$ and $e \geq 1$. We refer the reader to Waterhouse [17] for these and further details about abelian varieties.

Given an abelian variety A of dimension g defined over $\mathbb{F}_q$, for a prime $\ell \neq p$ one defines $A[\ell]$ as the group of points on A (with values in an algebraic closure $\bar{k}$) of order dividing ℓ. Like in the classical case over $\mathbb{C}$ it can be shown that $A[\ell]$ is a $2g$-dimensional $\mathbb{Z}/\ell\mathbb{Z}$-vector space. Things are different when $\ell = p$. The *p-rank* of A is defined by

$$r_p(A) = \dim_{\mathbb{F}_p} A[p](\bar{k}),$$

where $A[p](\bar{k})$ is the subgroup of p-torsion points over the algebraic closure. The p-rank can take any value between 0 and $g = \dim(A)$. When $r_p(A) = g$ we say that A is ordinary. The number $r_p(A)$ is invariant under isogenies over k, and satisfies $r_p(A_1 \times A_2) = r_p(A_1) + r_p(A_2)$.

The zeta function of C is defined by

$$Z_C(t) = exp\left(\sum_{n\geq 1} \#C(\mathbb{F}_{q^n})\frac{t^n}{n}\right) = exp\left(\sum_{n\geq 1} \#Fix(\pi^n)\frac{t^n}{n}\right).$$