Finite Fields and Their Applications 32 (2015) 207–232

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Counting curves over finite fields

Gerard van der Geer

Korteweg–de Vries Instituut, Universiteit van Amsterdam, Postbus 94248, 1090 GE Amsterdam, The Netherlands

ARTICLE INFO

Article history:
Received 25 August 2014
Received in revised form 10 September 2014
Accepted 18 September 2014
Available online 4 November 2014
Communicated by H. Stichtenoth

MSC:
11G20
10D20
14G15
14H10

Keywords:
Curve
Finite field
Modular form
Moduli of curves
Cohomology

ABSTRACT

This is a survey on recent results on counting of curves over finite fields. It reviews various results on the maximum number of points on a curve of genus g over a finite field of cardinality q, but the main emphasis is on results on the Euler characteristic of the cohomology of local systems on moduli spaces of curves of low genus and its implications for modular forms.

1. Introduction

Reduction modulo a prime became a standard method for studying equations in integers after Gauss published his Disquisitiones Arithmeticae in 1801. In §358 of the Disquisitiones Gauss counts the number of solutions of the cubic Fermat equation

E-mail address: G.B.M.vanderGeer@uva.nl.

http://dx.doi.org/10.1016/j.ffa.2014.09.008
1071-5797/© 2014 Elsevier Inc. All rights reserved.

$x^3 + y^3 + z^3 = 0$ modulo a prime p and finds for a prime $p \not\equiv 1 \pmod 3$ always $p + 1$ points on the projective curve, while for a prime $p \equiv 1 \pmod 3$ the number of points equals $p + 1 + a$, if one writes $4p = a^2 + 27b^2$ with $a \equiv 1 \pmod 3$ and he notes that $|a| \leq 2\sqrt{p}$. But although Galois introduced finite fields in 1830 and algebraic curves were one of the main notions in 19th century mathematics, one had to wait till the beginning of the 20th century before algebraic curves over finite fields became an important topic for mathematical investigation. Artin considered in his 1924 thesis (already submitted to Mathematische Zeitschrift in 1921) the function fields of hyperelliptic curves defined over a finite field and considered for such fields a zeta function $Z(s)$ that is an analogue of the Riemann zeta function and of the Dedekind zeta function for number fields. He derived a functional equation for them and formulated an analogue of the Riemann hypothesis that says that the zeros of the function of t obtained by substituting $t = q^{-s}$ in $Z(s)$ have absolute value $q^{-1/2}$. In 1931 Friedrich Karl Schmidt brought a more geometric approach by writing the zeta function for a smooth absolutely irreducible projective curve C over a finite field $\mathbb{F}_q$ as the generating function for the number of rational points $c(n) = \#C(\mathbb{F}_{q^n})$ over extension fields as

$$Z(t) = \exp\left(\sum_{n=1}^{\infty} c(n)\frac{t^n}{n}\right),$$

which turns out to be a rational function of t of the form

$$Z(t) = \frac{P(t)}{(1-t)(1-qt)}$$

for some polynomial $P \in \mathbb{Z}[t]$ of degree $2g$ with g the genus of the curve. He observed that the functional equation $Z(1/qt) = q^{1-g}t^{2-2g}Z(t)$ is a consequence of the theorem of Riemann–Roch. A couple of years later (1934) Hasse proved the Riemann hypothesis for elliptic curves over finite fields using correspondences. The proof appeared in 1936, see [29]. Deuring observed then that to extend this result to curves of higher genus one needed a theory of algebraic correspondences over fields of arbitrary characteristic. This was at the time that the need was felt to build algebraic geometry on a more solid base that would allow one to do algebraic geometry over arbitrary fields. Weil was one of those who actively pursued this goal. Besides doing foundational work, he also exploited the analogy between geometry in characteristic zero and positive characteristic by extending an inequality on correspondences of Castelnuovo and Severi to positive characteristic and deduced around 1940 the celebrated Hasse–Weil inequality

$$\big|\#C(\mathbb{F}_q) - (q+1)\big| \leq 2g\sqrt{q}$$

for the number of rational points on a smooth absolutely irreducible projective curve C of genus g over a finite field $\mathbb{F}_q$ [51].