Discrete Mathematics 340 (2017) 1327–1334

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On a number of rational points on a plane curve of low degree

Eun Ju Cheon [a], Masaaki Homma [b], Seon Jeong Kim [a,*], Namyong Lee [c]

[a] Department of Mathematics and RINS, Gyeongsang National University, Jinju 660-701, Republic of Korea
[b] Department of Mathematics and Physics, Kanagawa University, Hiratsuka 259-1293, Japan
[c] Department of Mathematics and Statistics, Minnesota State University, Mankato, MN 56001, USA

ARTICLE INFO

Article history:
Received 8 October 2015
Received in revised form 9 November 2016
Accepted 16 January 2017
Available online 3 March 2017

Keywords:
Finite field
Plane curve
Rational point

ABSTRACT

In Homma and Kim (2010), an upper bound of the number of rational points on a plane curve of degree d over $\mathbb{F}_q$ is found. Some examples attaining the bound are given in Homma and Kim (2010), whose degrees are $q+2, q+1, q, q-1, \sqrt{q}-1$ (when q is a square), and 2. In this paper, we consider an actual upper bound on such numbers for curves of low degree for $q \leq 7$. Also we give explicit examples of curves attaining the sharp bound for each d and q.

1. Introduction and preliminaries

Let $\mathbb{F}_q$ be the finite field with q elements, and $\mathbb{P}^2 := \mathbb{P}^2(\bar{\mathbb{F}}_q)$ the projective plane over the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$. We denote by $\mathbb{P}^2(\mathbb{F}_q) = \{(\alpha, \beta, \gamma) \in \mathbb{P}^2 \mid \alpha, \beta, \gamma \in \mathbb{F}_q\}$, the set of $\mathbb{F}_q$-rational points or simply $\mathbb{F}_q$-points over $\mathbb{F}_q$. Let C be an algebraic curve on $\mathbb{P}^2$ defined by a homogeneous equation $f(x, y, z) = 0$ whose coefficients are in $\mathbb{F}_q$, and $C(\mathbb{F}_q) = \{(\alpha, \beta, \gamma) \in \mathbb{P}^2(\mathbb{F}_q) \mid f(\alpha, \beta, \gamma) = 0\}$. We denote by $N_q(C) = {}^{\#}C(\mathbb{F}_q)$, the number of $\mathbb{F}_q$-points on C. For a curve C of degree d, B. Segre [8] mentioned that $N_q(C) \leq dq + 1$ and the equality holds if and only if C splits into d distinct lines. In this paper, we are interested in the value $N_q(C)$ for a curve C with no $\mathbb{F}_q$-linear component. We need not suppose that C is irreducible or nonsingular. The second and the third authors proved the following theorem.

Theorem 1 ([5, Theorem 3.1]). *If C is a plane curve of degree $d \geq 2$ over $\mathbb{F}_q$ without an $\mathbb{F}_q$-linear component, then the number of $\mathbb{F}_q$-points is bounded by*

$$N_q(C) \leq (d-1)q + 1,$$

unless C is a curve over $\mathbb{F}_4$ which is projectively equivalent to the curve defined by the following equation

$$x^4 + y^4 + z^4 + x^2y^2 + y^2z^2 + z^2x^2 + x^2yz + xy^2z + xyz^2 = 0, \tag{1}$$

which has $14 (= (d-1)q + 2)$ $\mathbb{F}_4$-points.

We denote by $M_q(d)$ the maximum of $N_q(C)$ where C is a plane curve of degree d with no $\mathbb{F}_q$-linear component. Then the above theorem says that $M_q(d) \leq (d-1)q + 1$ for every q and $d \geq 2$ except for $(q, d) = (4, 4)$. In [4], they give some examples of curves of degree $q+2, q+1, q, q-1, \sqrt{q}-1$ (when q is a square), and 2 which attain the bound. Thus for such degrees, the

* Corresponding author.
E-mail addresses: enju1000@naver.com (E.J. Cheon), homma@kanagawa-u.ac.jp (M. Homma), skim@gnu.kr (S.J. Kim), namyong.lee@mnsu.edu (N. Lee).

http://dx.doi.org/10.1016/j.disc.2017.01.017

bound is sharp. Now we want to know the sharp bound for each degree other than them. If the degree is bigger than $q+2$, then the sharp bound is $q^2+q+1 = {}^{\#}\mathbb{P}^2(\mathbb{F}_q)$ and examples are given in Proposition 1.1 in [3]. Note that every absolutely irreducible plane curve of degree 2, which we call a conic, over $\mathbb{F}_q$ contains $q+1$ $\mathbb{F}_q$-points. Thus we are concentrated on the degrees d with $3 \le d \le q-2$. For $q = 2, 3, 4$, we are done. Note that, for $q = 4$ and $d = 4$, the sharp bound is 14 as we stated in above theorem. For $q = 5$, only the case $d = 3$ is remained, and for $q = 7$, the cases $d = 3, 4, 5$ are remained. Thus we may consider only the cases $(q, d) = (5, 3)$ or $(7, 3)$ or $(7, 4)$ or $(7, 5)$.

R. Schoof [7] determined the number of projectively inequivalent nonsingular plane cubic curves over $\mathbb{F}_q$ with a given number of $\mathbb{F}_q$-points. K.-O. Stöhr and J.F. Voloch [9] proved the Stöhr–Voloch bound, that is, ${}^{\#}C(\mathbb{F}_q) \le \frac{1}{2}d(d+q-1)$ for a nonsingular and Frobenius classical C of degree d. The Stöhr–Voloch bound is effective even for an irreducible Frobenius classical curve C with singularities. For reader's convenience, we give its proof below. We remark that any curves over $\mathbb{F}_q$ are Frobenius classical for a prime number q.

Lemma 2 (*The Stöhr–Voloch Bound for Irreducible Curves*)**.** *If C is absolutely irreducible and Frobenius classical curve of degree $d \ge 2$ on the projective plane over $\mathbb{F}_q$, then we have $N_q(C) \le \frac{1}{2}d(d+q-1)$.*

Proof. Let $F(x_0, x_1, x_2) = 0$ be a defining equation of C. Let C' be another curve with the equation $F_0x_0^q + F_1x_1^q + F_2x_2^q = 0$, where F_i is the partial derivative of F with respect to x_i. For a nonsingular $\mathbb{F}_q$-point P on C, comparing the equations of C' and the tangent line of C at P, we know P is also contained in C'. By easy computation, we know that the tangent line of C' at P is equal to that of C. Thus the intersection multiplicity of C and C' at P, $I(C, C'; P)$ is at least two. For a singular $\mathbb{F}_q$-point P, since $F_0(P) = F_1(P) = F_2(P) = 0$, P is contained in C'. Since P is a singular point of C, we have $I(C, C'; P) \ge 2$. Note that C is irreducible and Frobenius classical, C is not a component of C'. Thus we have $|C(\mathbb{F}_q)| \le \frac{1}{2}\sum_{P\in C\cap C'} I(C, C'; P) \le \frac{1}{2}(\deg C)\cdot(\deg C') = \frac{1}{2}d(d+q-1)$. □

The following lemma is a corollary of the Sziklai bound, which guarantees a plane curve without $\mathbb{F}_q$-linear components having many $\mathbb{F}_q$-points to be absolutely irreducible.

Lemma 3. *Let C be a curve over $\mathbb{F}_q$ of degree $d \ge 2$ in $\mathbb{P}^2$ without $\mathbb{F}_q$-linear components. If $N_q(C) \ge (d-2)q+3$, then C is absolutely irreducible.*

Proof. See [6, Corollary 2.2]. □

We need some notations. For a nonnegative integer i, we call an $\mathbb{F}_q$-line ℓ an i-line of the curve C if ℓ contains exactly i points in $C(\mathbb{F}_q)$, and a_i denotes the number of i-lines on the projective plane. For a point $P \in \mathbb{P}^2(\mathbb{F}_q)$, P is said to be of type $i_1^{r_1}\dots i_t^{r_t}$ $(i_1 > \cdots > i_t \ge 0;\ r_1, \dots, r_t \ge 0)$ if the number of i_j-lines through P is r_j $(j = 1, \dots, t)$. The spectrum of C is defined to be the sequence of integers $(a_0, a_1, \dots, a_{q+1})$. We denote $\theta_n(q) := {}^{\#}\mathbb{P}^n(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$. Note that $\sum_{j=0}^{q+1} r_j = q+1$, $\sum_{j=0}^{q+1} r_j i_j = N_q(C)$ for $P \in \mathbb{P}^2(\mathbb{F}_q) \setminus C(\mathbb{F}_q)$ [resp. $\sum_{j=0}^{q+1} r_j(i_j - 1) + 1 = N_q(C)$ for $P \in C(\mathbb{F}_q)$], and $\sum_{j=0}^{q+1} a_i = \theta_2(q)$.

2. The case $d = 3$ or 4

In this section we give the sharp bounds for cases $(q, d) = (5, 3), (7, 3), (7, 4)$. Some examples are found by elementary computation using Maple 16.

2.1. $M_5(3) = 10$ *and* $M_7(3) = 13$

Let C be a curve of degree 3 without $\mathbb{F}_q$-linear component. If C is not absolutely irreducible, by Lemma 3, $N_q(C) \le q+2$. If C is absolutely irreducible, by Lemma 2, $N_q(C) \le \frac{3}{2}(q+2)$. Thus $M_5(3) \le 10$ [resp. $M_7(3) \le 13$]. For nonsingular curves C, using Schoof's result [7], we also know that there is a unique (up to projective equivalence) nonsingular plane cubic curve with 10 $\mathbb{F}_5$-points [resp. 13 $\mathbb{F}_7$-points] as well as $M_5(3) \le 10$ [resp. $M_7(3) \le 13$]. Using elementary computation by Maple 16, we could find irreducible cubics with 10 $\mathbb{F}_5$-points [resp. 13 $\mathbb{F}_7$-points], which are projectively equivalent to each other, so we give one as follows;

$$2x^3 + 4x^2y + 3y^3 + x^2z + 2xz^2 [\text{resp. } 3y^3 + 4x^2z + xz^2 + 6z^3],$$

whose spectrum is $(a_0, a_1, a_2, a_3) = (4, 6, 9, 12)$ [resp. $(a_0, a_1, a_2, a_3) = (9, 14, 12, 22)$]. Thus $M_5(3) = 10$ and $M_7(3) = 13$.

2.2. $M_7(4) = 20$

Let C be a curve of degree 4 without $\mathbb{F}_7$-linear component. If C is not absolutely irreducible, by Lemma 3, $N_q(C) \le 16$. If C is absolutely irreducible over $\mathbb{F}_7$, then by Lemma 2, $N_q(C) \le 20$. Using elementary computation by Maple 16, we could find curves of degree 4 with 20 $\mathbb{F}_7$-points, which must be absolutely irreducible, as follows;

$$6x^3y + 3x^2y^2 + 5xy^3 + 5x^3z + 5x^2yz + 3y^3z + 2x^2z^2 + 6xz^3 + 4yz^3 = 0,$$