Séminaires & Congrès
11, 2005, p. 75–110

ON CURVES OVER FINITE FIELDS

by

Arnaldo Garcia

***Abstract.* —** In these notes we present some basic results of the Theory of Curves over Finite Fields. Assuming a famous theorem of A. Weil, which bounds the number of solutions in a finite field (*i.e.*, number of rational points) in terms of the genus and the cardinality of the finite field, we then prove several other related bounds (bounds of Serre, Ihara, Stohr-Voloch, etc.). We then treat Maximal Curves (classification and genus spectrum). Maximal curves are the curves attaining the upper bound of A. Weil. If the genus of the curve is large with respect to the cardinality of the finite field, Ihara noticed that Weil's bound cannot be reached and he introduced then a quantity $A(q)$ for the study of the asymptotics of curves over a fixed finite field. This leads to towers of curves and we devote special attention to the so-called recursive towers of curves. We present several examples of recursive towers with good asymptotic behaviour, some of them attaining the Drinfeld-Vladut bound. The connection with the asymptotics of linear codes is a celebrated result of Tsfasman-Vladut-Zink, which is obtained via Goppa's construction of codes from algebraic curves over finite fields.

***Résumé* (Courbes sur des corps finis). —** Nous présentons des résultats élémentaires sur les courbes sur les corps finis et leurs points rationnels. Nous avons fait un effort pour donner une présentation aussi simple que possible, la rendant accessible aux non spécialistes. Parmi ces résultats se trouvent : le théorème de Weil (l'hypothèse de Riemann dans ce contexte), son amélioration donnée par Serre, la borne de Ihara sur le genre pour les courbes maximales, genre et classification des courbes maximales, théorie de Stohr-Voloch des ordres de Frobenius pour les courbes planes, constructions de courbes sur les corps finis ayant beaucoup de points rationnels, les formules explicites de Serre, étude asymptotique des courbes sur les corps finis et des codes correcteurs d'erreurs (la connexion entre elles est un célèbre théorème de Tsfasman-Vladut-Zink), tours récursives de courbes et certaines tours particulièrement intéressantes (atteignant la borne de Drinfeld-Vladut sur des corps finis de cardinal un carré ou atteignant la borne de Zink sur des corps finis de cardinal un cube).

2000 *Mathematics Subject Classification.* — 14H05, 11G20 , 14G05.
***Key words and phrases.* —** Algebraic curves, finite fields, rational points, genus, linear codes, asymptotics, tower of curves.

The author was partially supported by PRONEX # 662408/1996-3 (CNPq-Brazil).

1. Introduction

These notes reflect very closely the lectures given by the author at a "European School on Algebraic Geometry and Information Theory", held at C.I.R.M. – Luminy - France in May 2003. They are intended as an invitation to the subject of curves over finite fields. At several points we have sacrificed rigorness (without mention) in favour of clarity or simplicity. Assuming to start with a very deep theorem of André Weil (equivalent to the validity of Riemann's Hypothesis for the situation of zeta functions associated to nonsingular projective curves over finite fields) we then prove several interesting related results with elementary methods (bounds of Serre, Ihara, Stöhr-Voloch, Drinfeld-Vladut, etc.), and we give also several examples illustrating those results.

These notes are organized as follows: Section 2 contains several bounds on the number of rational points of curves over finite fields (see Theorems 2.2, 2.3, 2.14 and 2.17) and examples of curves attaining those bounds. Specially interesting here are the curves attaining Weil's bound, the so-called *maximal curves*; for these curves there is a genus bound due to Ihara (see Proposition 2.8) which originated two basic problems on maximal curves: the genus spectrum problem (see Theorem 2.11) and the classification problem (see Theorems 2.10 and 2.12). For the classification problem a very important tool is the Stöhr-Voloch theory of Frobenius – orders of morphisms of curves over finite fields, and this theory is illustrated here just for projective plane curves (see Theorem 2.17). Section 3 contains two simple and related methods for the construction of curves with many rational points with respect to the genus (called *good curves*). Both constructions lead to projective curves that are Kummer covers of the projective line (or of another curve), and we also present a "recipe" due to Hasse for the genus calculation for such covers. Several examples illustrating both constructions are also presented.

Section 4 explains the basic facts on the asymptotic behaviour of curves and also of linear codes over finite fields. The relation between the two asymptotics (of curves and of codes) is a result due to Tsfasman-Vladut-Zink and this result represents an improvement on the so-called Gilbert-Varshamov bound. We also prove here an asymptotic bound due to Drinfeld-Vladut (see Proposition 4.3) which is obtained as an application of a method of Serre (see Theorem 4.1). This motivates the definition of towers of curves over finite fields which is the subject of Section 5. After introducing the concepts of ramification locus and splitting locus, we explain their significance when the tower is a tame tower (see Theorem 5.1). We then define recursive towers and we give several examples illustrating applications of Theorem 5.1. Wild towers are much harder to deal with than tame towers, and we give at the end of these notes two very interesting examples of wild towers (see Examples 5.8 and 5.9). Example 5.9 is specially interesting since it is over finite fields with cubic cardinalities, and it

gives in particular a generalization of a famous lower bound, on the asymptotics of curves, due to T. Zink.

2. Bounds for the number of rational points

Let $f(X,Y) \in \mathbb{F}_q[X,Y]$ be an absolutely irreducible polynomial (*i.e.*, $f(X,Y)$ is also irreducible over $\overline{\mathbb{F}}_q$ the algebraic closure of the finite field $\mathbb{F}_q$). The associated affine plane curve $\mathcal{C}$ is defined by

$$\mathcal{C} := \{(a,b) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q \mid f(a,b) = 0\}$$

and we denote by $\mathcal{C}(\mathbb{F}_q)$ the set of rational points; *i.e.*,

$$\mathcal{C}(\mathbb{F}_q) = \{(a,b) \in \mathcal{C} \mid a,b \in \mathbb{F}_q\}.$$

Goal. — *Study the cardinality $\#\mathcal{C}(\mathbb{F}_q)$ with respect to the genus $g(\mathcal{C})$.*

The genus $g(\mathcal{C})$ of a plane curve $\mathcal{C}$ satisfies

$$g(\mathcal{C}) \leqslant (d-1)(d-2)/2,$$

where $d := \deg f(X,Y)$ is the degree of the irreducible polynomial defining the curve $\mathcal{C}$.

The next lemma gives a simple criterion for absolute irreducibility.

***Lemma 2.1* (See [27])**. — *Let $f(X,Y) \in \mathbb{F}_q[X,Y]$ be a polynomial of the following type*

$$f(X,Y) = a_0 \cdot Y^n + a_1(X) \cdot Y^{n-1} + \cdots + a_{n-1}(X) \cdot Y + a_n(X)$$

with $a_0 \in \mathbb{F}_q^*$ and with $a_1(X), \ldots, a_{n-1}(X)$, $a_n(X) \in \mathbb{F}_q[X]$.

Suppose that $\gcd(n, \deg a_n(X)) = 1$ *and that*

$$\frac{\deg a_n(X)}{n} > \frac{\deg a_i(X)}{i} \quad \textit{for each } 1 \leqslant i \leqslant n-1,$$

then the polynomial $f(X,Y)$ is absolutely irreducible.

We are going to deal with more general algebraic curves, not just an affine plane curve. Given $n-1$ polynomials $f_1(X_1, \ldots, X_n)$, $f_2(X_1, \ldots, X_n), \ldots, f_{n-1}(X_1, \ldots, X_n)$ in the polynomial ring $\mathbb{F}_q[X_1, \ldots, X_n]$, they in general define an affine algebraic curve $\mathcal{C}$ as

$$\mathcal{C} := \{(a_1, a_2, \ldots, a_n) \in \overline{\mathbb{F}}_q^n \mid f_j(a_1, \ldots, a_n) = 0 \quad \text{for all } j = 1, 2, \ldots, n-1\}$$

and its set $\mathcal{C}(\mathbb{F}_q)$ of rational points as $\mathcal{C}(\mathbb{F}_q) := \{(a_1, \ldots, a_n) \in \mathcal{C} \mid a_1, a_2, \ldots, a_n \in \mathbb{F}_q\}$.

A point P of a curve $\mathcal{C}$ is called *nonsingular* if there exists a tangent line to the curve $\mathcal{C}$ at the point P. For example if $P = (a,b) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ is a point of the plane curve associated to the polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ (*i.e.*, if we have $f(a,b) = 0$), then the point P is called *nonsingular* when

$$f_X(a,b) \neq 0 \quad \text{or} \quad f_Y(a,b) \neq 0,$$

where f_X and f_Y denote the partial derivatives. The curve $\mathcal{C}$ is called *nonsingular* if every point $P \in \mathcal{C}$ is a nonsingular point. Also, we will deal with projective curves here rather than with affine curves. For example, if $\mathcal{C}$ is the plane curve associated to the polynomial $f(X,Y)$ in $\mathbb{F}_q[X,Y]$ with $d := \deg f(X,Y)$, then we define

$$F(X,Y,Z) = Z^d \cdot f\,(X/Z, Y/Z) \quad \text{and} \quad \widetilde{\mathcal{C}} := \{(a:b:c) \in \mathbb{P}^2(\overline{\mathbb{F}}_q) \mid F(a,b,c) = 0\}.$$

The curve $\widetilde{\mathcal{C}}$ is a projective model for the affine curve $\mathcal{C}$ associated to $f(X,Y)$. If the projective plane curve $\widetilde{\mathcal{C}}$ is nonsingular, then we have the equality $g(\widetilde{\mathcal{C}}) = (d-1)(d-2)/2$. A point $(a:b:c)$ of $\widetilde{\mathcal{C}}$ is said to be *at infinity* when $c = 0$.

The next theorem is due to A. Weil and it is the main result in this theory:

***Theorem 2.2* (See [33] and [30], Theor. V.2.3).** — *Let $\mathcal{C}$ be a projective and nonsingular, absolutely irreducible curve defined over the finite field $\mathbb{F}_q$ with q elements. Then we have*

$$\#\mathcal{C}(\mathbb{F}_q) \leqslant 1 + q + 2\sqrt{q} \cdot g(\mathcal{C}).$$

Theorem 2.2 is a very deep result. It was proved in the particular case of elliptic curves (*i.e.*, the case $g(\mathcal{C}) = 1$) by H. Hasse and in the general case by A. Weil (see [**33**]). Theorem 2.2 says that the zeros of a certain "Congruence Zeta Function" (associated to the curve by E. Artin in analogy with Dedekind's Zeta Function for quadratic number fields) all lie on the critical line $\mathrm{Re}(s) = 1/2$. We can rewrite Theorem 2.2 as follows

***Theorem 2.3* (See [33] and [30], Cor. V.1.16).** — *Let $\mathcal{C}$ be a projective and nonsingular, absolutely irreducible algebraic curve defined over $\mathbb{F}_q$ and let $g := g(\mathcal{C})$ denote its genus. Then there exist algebraic integers $\alpha_1, \alpha_2, \ldots, \alpha_{2g} \in \mathbb{C}$ with absolute value $|\alpha_j| = \sqrt{q}$, for $1 \leqslant j \leqslant 2g$, such that*

$$\#\mathcal{C}(\mathbb{F}_q) = q + 1 - \sum_{j=1}^{2g} \alpha_j.$$

Clearly, the bound in Theorem 2.2 follows from the equality in Theorem 2.3 by taking $\alpha_j = -\sqrt{q}$, for all values of j with $1 \leqslant j \leqslant 2g$. We now define

***Definition 2.4*.** — Let $q = \ell^2$ be a square. We say that the curve $\mathcal{C}$ is $\mathbb{F}_q$-*maximal* if it attains the bound in Theorem 2.2; *i.e.*, if it holds that

$$\#\mathcal{C}(\mathbb{F}_q) = \ell^2 + 1 + 2\ell \cdot g(\mathcal{C}).$$

***Example 2.5* (Hermitian curve over $\mathbb{F}_{\ell^2}$).** — Consider the projective plane curve $\mathcal{C}$ defined over the finite field $\mathbb{F}_{\ell^2}$ by the affine equation

$$f(X,Y) = Y^\ell + Y - X^{\ell+1} \in \mathbb{F}_{\ell^2}[X,Y].$$

We have $g(\mathcal{C}) = \ell(\ell-1)/2$; indeed, the curve $\mathcal{C}$ is a nonsingular plane curve with degree d satisfying $d = \ell + 1$. The number of $\mathbb{F}_q$-rational points (with $q = \ell^2$) is given by

$$\#\mathcal{C}(\mathbb{F}_q) = 1 + \ell^3 = 1 + \ell^2 + 2\ell \cdot \frac{\ell(\ell-1)}{2};$$

i.e., the curve $\mathcal{C}$ is $\mathbb{F}_{\ell^2}$-maximal. Indeed, the associated homogeneous polynomial is

$$F(X, Y, Z) = Y^\ell Z + Y Z^\ell - X^{\ell+1}$$

and the point $(0 : 1 : 0)$ is the unique point at infinity on the curve $\mathcal{C}$. The affine points are the points $(a, b) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ such that

$$b^\ell + b = a^{\ell+1}.$$

Observing that $a^{\ell+1}$ is the norm for the extension $\mathbb{F}_{\ell^2}/\mathbb{F}_\ell$ and that $b^\ell + b$ is the trace for $\mathbb{F}_{\ell^2}/\mathbb{F}_\ell$, we conclude that

$$\#\mathcal{C}(\mathbb{F}_{\ell^2}) = 1 + \ell^3. \qquad \square$$

The next proposition, due to J.-P. Serre, enables one to construct other $\mathbb{F}_q$-maximal curves from known ones.

***Proposition 2.6* (See [26])**. — *Let $\varphi\colon \mathcal{C} \to \mathcal{C}_1$ be a surjective morphism defined over a finite field $\mathbb{F}_q$ (i.e., both curves $\mathcal{C}$ and $\mathcal{C}_1$, and also the map φ are all defined over the finite field $\mathbb{F}_q$) and suppose that the curve $\mathcal{C}$ is $\mathbb{F}_q$-maximal. Then the curve $\mathcal{C}_1$ is also $\mathbb{F}_q$-maximal.*

Example 2.7. — Let $\mathcal{C}_1$ be the curve defined over $\mathbb{F}_{\ell^2}$ by the following equation

$$f(X, Y) = Y^\ell + Y - X^m, \qquad \text{with } m \text{ a divisor of } \ell + 1.$$

This curve $\mathcal{C}_1$ is $\mathbb{F}_{\ell^2}$-maximal. Indeed, this follows from Proposition 2.6 since we have the following surjective morphism (with $n := (\ell+1)/m$)

$$\begin{aligned} \varphi\colon \mathcal{C} &\longrightarrow \mathcal{C}_1 \\ (a, b) &\longmapsto (a^n, b), \end{aligned}$$

where the curve $\mathcal{C}$ is the one given in Example 2.5.

The genus of $\mathcal{C}_1$ satisfies (see Example 3.1 in Section 3)

$$g(\mathcal{C}_1) = (\ell-1)(m-1)/2.$$

One can check directly that the curve $\mathcal{C}_1$ is $\mathbb{F}_q$-maximal with $q = \ell^2$. Indeed, let us denote by H the multiplicative subgroup of $\mathbb{F}_{\ell^2}^*$ with order $|H| = (\ell-1) \cdot m$. We then have:

(1) $$a \in H \cup \{0\} \text{ implies that } a^m \in \mathbb{F}_\ell.$$

Since $b^\ell + b = a^m$ for an affine point $(a, b) \in \mathcal{C}_1$ and since $b^\ell + b$ is the trace for the extension $\mathbb{F}_{\ell^2}/\mathbb{F}_\ell$, we get from the assertion in (1) that

$$\#\mathcal{C}_1(\mathbb{F}_{\ell^2}) \geqslant 1 + [1 + m(\ell-1)] \cdot \ell.$$