manuscripta math. 88, 467 - 478 (1995)

manuscripta mathematica

Coverings of Singular Curves over Finite Fields

Yves Aubry[1], **Marc Perret**[2]

[1] Département de Mathématiques, Université de Caen
Esplanade de la Paix - 14 032 Caen Cedex - France.

[2] Unité de Mathématiques, École Normale Supérieure de Lyon
46, allée d'Italie - 69 363 Lyon Cedex 7 - France.

Received April 10, 1995;
in revised form September 14, 1995

We prove that if $f : Y \longrightarrow X$ is a finite flat morphism between two reduced absolutely irreducible algebraic projective curves defined over the finite field $\mathbb{F}_q$, then

$$| \sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q) | \leq 2(\pi_Y - \pi_X)\sqrt{q},$$

where π_C is the arithmetic genus of a curve C. As application, we give some character sum estimation on singular curves.

In this paper, the word *curve* stands for a reduced absolutely irreducible algebraic projective curve defined over the finite field $\mathbb{F}_q$ with q elements. If X is a smooth curve, it has been shown by Weil in [6] that the number of $\mathbb{F}_q$-rational points of X, denoted by $\sharp X(\mathbb{F}_q)$, is related to the geometric genus g_X by :

$$\mid \sharp X(\mathbb{F}_q) - (q+1) \mid \leq 2g_X\sqrt{q} \tag{1}$$

(with an improvement of Serre using the integral part, see [5]). In fact, Weil's statement, involving the zeta function of X, is more precise. It implies that if there is a finite morphism $f : Y \longrightarrow X$ between two smooth curves X and Y having (geometric) genus g_X and g_Y respectively, then (see for instance [2], proposition 6)

$$\mid \sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q) \mid \leq 2(g_Y - g_X)\sqrt{q}. \tag{2}$$

When X is the projective line, this is exactly Weil's bound for Y.

On the other hand, the authors proved in [1] that if X is a singular curve, then Weil's inequality (1) holds if one replaces the geometric genus g_X of X by its arithmetic genus π_X. The aim of this paper is to give a generalization of both (2) and (1) for singular curves. Namely, if $f : Y \longrightarrow X$ is a finite flat morphism between two singular curves, then

$$\mid \sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q) \mid \leq 2(\pi_Y - \pi_X)\sqrt{q} \tag{3}$$

holds.

We will prove (3) in the third section. The proof goes as follows. Inequality (2) can be applied to the finite morphism $\tilde{f} : \tilde{Y} \longrightarrow \tilde{X}$ induced by f on the smooth models of X and Y respectively. Furthermore the number of $\mathbb{F}_q$-rational points of a curve is related to the number of $\mathbb{F}_q$-rational points of its smooth model (first section). Unfortunately, this is not sufficient to prove (3). One has to introduce (in the second section) the auxiliary curve $Z = \tilde{X} \times_X Y$, birational to Y.

Finally, we apply this result in a fifth section to obtain some character sum estimations.

1. A lemma

The following lemma relates the number of $\mathbb{F}_q$-rational points of a curve and that of its smooth model. It is given in [1], but in order to be self contained, we give here its short proof. If P is a $\mathbb{F}_q$-rational point of a curve X, we denote by α_P (respectively $\alpha_P(\infty)$) the number of $\mathbb{F}_q$-rational points (respectively of $\overline{\mathbb{F}}_q$-rational points, where $\overline{\mathbb{F}}_q$ stands for an algebraic closure of $\mathbb{F}_q$) of $\tilde{X}$, lying over P in the normalization map $\nu_X : \tilde{X} \longrightarrow X$. Let $\mathcal{O}_P$ be the local ring of X at P, and $\overline{\mathcal{O}_P}$ its integral closure in the function field $\mathbb{F}_q(X)$ of X. The quotient $\overline{\mathcal{O}_P}/\mathcal{O}_P$ is a $\mathbb{F}_q$-vector space of finite length : let δ_P be its dimension.

Lemma 1. *Let X be a reduced absolutely irreducible projective algebraic curve defined over $\mathbb{F}_q$. Then*

$$| \sharp\tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q) | \leq \sum_{P \in X(\mathbb{F}_q)} | \alpha_P - 1 | \leq \pi_X - g_X.$$

Proof. Let us first prove that if P is a $\mathbb{F}_q$-rational singular point of X, then $\alpha_P - 1 \leq \delta_P$. Let $Q_1, \ldots, Q_{\alpha_P(\infty)}$ be the $\overline{\mathbb{F}}_q$-rational points of $\tilde{X}$ lying over P (the α_P first beeing the $\mathbb{F}_q$-rational ones), and ϕ the $\mathbb{F}_q$-linear map

$$\begin{array}{cccc} \phi : & \overline{\mathcal{O}_P} & \longrightarrow & {\mathbb{F}_q}^{\alpha_P} \\ & f & \longmapsto & \big(f(Q_i)\big)_{1 \leq i \leq \alpha_P} \end{array}$$

We prove that ϕ is onto : let $(x_1, \ldots, x_{\alpha_P}) \in {\mathbb{F}_q}^{\alpha_P}$ and $f_i = x_i \in \mathbb{F}_q \subset \mathbb{F}_q(X)$ if $i \leq \alpha_P$. For $i \geq \alpha_P + 1$, let $f_i = 0$. Then by the weak approximation theorem, there exists $g \in \mathbb{F}_q(X)$ such that $v_{Q_i}(g - f_i) \geq 1$ for $1 \leq i \leq \alpha_P(\infty)$. Hence, $\phi(g) = (x_1, \ldots, x_{\alpha_P})$ and

$$g \in \bigcap_{1 \leq i \leq \alpha_P(\infty)} \mathcal{O}_{Q_i} = \overline{\mathcal{O}_P}.$$

Since $f(Q_1) = \cdots = f(Q_{\alpha_P})$ for $f \in \mathcal{O}_P$, it follows that $\phi(\mathcal{O}_P)$ is contained in the vector-line $L \subset {\mathbb{F}_q}^{\alpha_P}$ spanned by $(1, ..., 1)$. One obtains a surjective linear map

$$\tilde{\phi} : \overline{\mathcal{O}_P}/\mathcal{O}_P \longrightarrow {\mathbb{F}_q}^{\alpha_P}/L.$$

Taking dimensions, we obtain that $\alpha_P - 1 \leq \delta_P$.

Now, Lemma 1 follows from the formulas

$$\pi_X - g_X = \sum_{P \in \operatorname{Sing} X(\overline{\mathbb{F}}_q)} \delta_P$$

and

$$\sharp\tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q) = \sum_{P \in X(\mathbb{F}_q)} (\alpha_P - 1).$$

□

2. An auxiliary curve

Let X and Y be two curves, and $f : Y \longrightarrow X$ be a finite flat morphism. In order to give an estimate for the difference between the numbers of $\mathbb{F}_q$-rational points of X and Y, it is convenient to consider the fibre product $Z = \tilde{X} \times_X Y$.

Lemma 2. *Z is a reduced absolutely irreducible projective curve.*

Proof. The map f beeing finite, the map $Z \longrightarrow \tilde{X}$ is finite and onto, which implies that $\dim Z = \dim \tilde{X} = 1$, and Z is a curve.

In order to prove that Z is absolutely integral, one has to prove that given an affine open set $\operatorname{Spec} A(X_i)$ of X, the ring $A = \overline{A(X_i)} \otimes_{A(X_i)} A(Y_i)$ is an integral domain, where $\bar{A}$ stands for the integral closure of a ring A, and $A(Y_i)$ is defined by $\operatorname{Spec} A(Y_i) = f^{-1}(\operatorname{Spec} A(X_i))$. Denote by $\operatorname{Frac}(A)$ the quotient field of a domain A. By the flatness hypothesis,

$$0 \longrightarrow \overline{A(X_i)} \longrightarrow \operatorname{Frac}(A(X_i))$$

induce

$$0 \longrightarrow A \longrightarrow \mathrm{Frac}(A(X_i)) \otimes_{A(X_i)} A(Y_i).$$

Then, the injective map

$$\mathrm{Frac}(A(X_i)) \otimes_{A(X_i)} A(Y_i) \hookrightarrow \mathrm{Frac}(A(Y_i))$$

proves that A is an integral domain, as a subring of a field.

Finally, Z is projective. Indeed, f is proper since it is finite, and $Z \longrightarrow \tilde{X}$ is also proper, so that the composite morphism $Z \longrightarrow \tilde{X} \longrightarrow \operatorname{Spec} \mathbb{F}_q$ is proper since $\tilde{X}$ is complete. Hence, Z is projective as a complete curve. □

By the universal properties of the fibre product and of normalization maps, one can write the following diagram, where all triangles and squares are commutative, and all morphisms are finite :

$$\begin{tikzcd}
\tilde{Y} \arrow[dr] \arrow[drr, "\tilde{f}"] \arrow[ddr, "\nu_Y"'] & & \\
& Z \arrow[r] \arrow[d] & \tilde{X} \arrow[d, "\nu_X"] \\
& Y \arrow[r, "f"] & X
\end{tikzcd}$$

The sheaf of $\mathcal{O}_X$-modules $f_*\mathcal{O}_Y$ is coherent because f is finite. It is then locally free since f is flat. After localization, the stalks $(f_*\mathcal{O}_Y)_P$ are $\mathcal{O}_{X,P}$-module of finite type, whose rank doesn't depend on P since X is connected. Let

$$\begin{aligned} r &= \dim_{\mathbb{F}_q(P)}(f_*\mathcal{O}_Y)_P \otimes_{\mathcal{O}_{X,P}} \mathbb{F}_q(P) \\ &= \sum_{Q \in f^{-1}(P)} \dim_{\mathbb{F}_q(P)}(\mathcal{O}_{Y,Q} \otimes_{\mathcal{O}_{X,P}} \mathbb{F}_q(P)) \end{aligned}$$

be this rank, where $\mathbb{F}_q(P)$ denotes the residue field of the point P. Note that if $r = 1$, then $f^{-1}(P) = \{Q\}$ contains only one element for any $P \in X$, and f induces a morphism of local rings $\mathcal{O}_{Y,Q} \longrightarrow \mathcal{O}_{X,P}$, so that f is an isomorphism. Hence, one can suppose $r \geq 2$.

Proposition 3. *(i) Z is birational to Y. In particular, $g_Z = g_Y$.*
(ii) The arithmetic genus of Z is given by

$$\pi_Z = \pi_Y - r(\pi_X - g_X).$$

Proof. (i) This is trivial since there are dominant morphisms $\tilde{Y} \longrightarrow Z$ and $Z \longrightarrow Y$.
(ii) Since both arithmetic and geometric genus of a curve C and of $C \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q = \overline{C}$ are the same, it is sufficient to compute $\pi_{\overline{Z}}$. To simplify notations, we continue to denote by X, Y and Z the curves $\overline{X}$, $\overline{Y}$ and $\overline{Z}$ respectively. The exact sequence of $\mathcal{O}_X$-module sheaves

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \nu_{X,*}\mathcal{O}_{\tilde{X}} \longrightarrow (\nu_{X,*}\mathcal{O}_{\tilde{X}})/\mathcal{O}_X \longrightarrow 0$$

tensorized by the flat $\mathcal{O}_X$-module $f_*\mathcal{O}_Y$, gives the exact sequence

$$\begin{aligned} 0 \longrightarrow f_*\mathcal{O}_Y \longrightarrow (\nu_{X,*}\mathcal{O}_{\tilde{X}}) \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y \longrightarrow \\ \longrightarrow \big((\nu_{X,*}\mathcal{O}_{\tilde{X}})/\mathcal{O}_X\big) \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y \longrightarrow 0 \end{aligned} \tag{4}$$

from which we deduce a long exact sequence of cohomology. Let us scrutinize its different terms.

Since $H^i(X, f_*\mathcal{O}_Y) \cong H^i(Y, \mathcal{O}_Y)$ and Y is projective, then we have $\dim_{\overline{\mathbb{F}}_q} H^0(X, f_*\mathcal{O}_Y) = 1$ and $\dim_{\overline{\mathbb{F}}_q} H^1(X, f_*\mathcal{O}_Y) = \pi_Y$. In the same way,

$$\dim_{\overline{\mathbb{F}}_q} H^0(X, (\nu_{X,*}\mathcal{O}_{\tilde{X}}) \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y) = 1$$

and

$$\dim_{\overline{\mathbb{F}}_q} H^1(X, (\nu_{X,*}\mathcal{O}_{\tilde{X}}) \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y) = \pi_Z.$$

Furthermore, the sheaf $(\nu_{X,*}\mathcal{O}_{\tilde{X}})/\mathcal{O}_X$ is a sum of skyscraper sheaves on the singular points of X. Hence, this is also the case for $\big((\nu_{X,*}\mathcal{O}_{\tilde{X}})/\mathcal{O}_X\big) \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y$, and this prove the vanishing of its H^1. Finally,

$$\begin{aligned}
&\dim_{\overline{\mathbb{F}}_q} H^0(X, \big((\nu_{X,*}\mathcal{O}_{\tilde{X}})/\mathcal{O}_X\big) \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y) \\
&= \sum_{P \in \operatorname{Sing} X(\overline{\mathbb{F}}_q)} \dim_{\overline{\mathbb{F}}_q} \big((\overline{\mathcal{O}_{X,P}}/\mathcal{O}_{X,P}) \otimes_{\mathcal{O}_{X,P}} (f_*\mathcal{O}_Y)_P\big) = \\
&\sum_{P \in \operatorname{Sing} X(\overline{\mathbb{F}}_q)} \dim_{\overline{\mathbb{F}}_q} \big((\overline{\mathcal{O}_{X,P}}/\mathcal{O}_{X,P}) \otimes_{\overline{\mathbb{F}}_q} (\overline{\mathbb{F}}_q \otimes_{\mathcal{O}_{X,P}} (f_*\mathcal{O}_Y)_P)\big) \\
&= \sum_{P \in \operatorname{Sing} X(\overline{\mathbb{F}}_q)} \dim_{\overline{\mathbb{F}}_q} \big((\overline{\mathcal{O}_{X,P}}/\mathcal{O}_{X,P}) \otimes_{\overline{\mathbb{F}}_q} (\overline{\mathbb{F}}_q)^r\big) \\
&= \sum_{P \in \operatorname{Sing} X(\overline{\mathbb{F}}_q)} \dim_{\overline{\mathbb{F}}_q} (\overline{\mathcal{O}_{X,P}}/\mathcal{O}_{X,P})^r \\
&= r(\pi_X - g_X).
\end{aligned}$$

The nullity of the alternating sum of the $\overline{\mathbb{F}}_q$-dimensions of the different terms of the long exact sequence of cohomology given by (4) gives :

$$1 - 1 + r(\pi_X - g_X) - \pi_Y + \pi_Z - 0 = 0,$$

which was to be proved. □

3. The main theorem

Theorem 4. *Let X and Y be two reduced absolutely irreducible projective algebraic curves defined over $\mathbb{F}_q$, with respective arithmetic genus π_X and π_Y, and let $f : Y \longrightarrow X$ be a finite flat morphism defined over $\mathbb{F}_q$. Then*

$$\mid \sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q) \mid \leq 2(\pi_Y - \pi_X)\sqrt{q}.$$

The proof depends on the following lemma.

Lemma 5.

$$\mid (\sharp Z(\mathbb{F}_q) - \sharp \tilde{X}(\mathbb{F}_q)) - (\sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)) \mid \leq (r-1)(\pi_X - g_X)$$

(recall that $r = \dim_{\mathbb{F}_q(P)}(f_*\mathcal{O}_Y)_P \otimes_{\mathcal{O}_{X,P}} \mathbb{F}_q(P)$).

Proof. If $P \in X(\mathbb{F}_q)$, let

$$\alpha_P = \sharp\{\tilde{P} \in \tilde{X}(\mathbb{F}_q) \mid \nu_X(\tilde{P}) = P\}$$

and

$$\beta_P = \sharp\{Q \in Y(\mathbb{F}_q) \mid f(Q) = P\}.$$

Then

$$\beta_P \leq \sum_{Q \in f^{-1}(P)} 1 \leq \sum_{Q \in f^{-1}(P)} \dim_{\mathbb{F}_q(P)} \left(\mathcal{O}_{Y,Q} \otimes_{\mathcal{O}_{X,P}} \mathbb{F}_q(P)\right) = r$$

Moreover,

$$Z(\mathbb{F}_q) = \{(\tilde{P}, Q) \in \tilde{X}(\mathbb{F}_q) \times Y(\mathbb{F}_q) \mid \nu_X(\tilde{P}) = f(Q)\}$$

hence

$$\begin{aligned}\sharp Z(\mathbb{F}_q) - \sharp \tilde{X}(\mathbb{F}_q) &= \sum_{P \in X(\mathbb{F}_q)} \alpha_P \beta_P - \sum_{P \in X(\mathbb{F}_q)} \alpha_P \\ &= \sum_{P \in X(\mathbb{F}_q)} \alpha_P(\beta_P - 1),\end{aligned}$$

and

$$\begin{aligned}\sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q) &= \sum_{P \in X(\mathbb{F}_q)} \beta_P - \sum_{P \in X(\mathbb{F}_q)} 1 \\ &= \sum_{P \in X(\mathbb{F}_q)} (\beta_P - 1).\end{aligned}$$

By lemma 1, and since $r \geq 2$, we obtain

$$\begin{aligned}
&| (\sharp Z(\mathbb{F}_q) - \sharp\tilde{X}(\mathbb{F}_q)) - (\sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)) | \leq \\
&\qquad \leq (r-1) \sum_{P \in X(\mathbb{F}_q)} | \alpha_P - 1 | \\
&\qquad \leq (r-1)(\pi_X - g_X).
\end{aligned}$$

□

The theorem follows easily from the preceding and the triangular inequality

$$\begin{aligned}
| \sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q) | \leq & | \sharp\tilde{Y}(\mathbb{F}_q) - \sharp Z(\mathbb{F}_q) | \\
& + | (\sharp Z(\mathbb{F}_q) - \sharp\tilde{X}(\mathbb{F}_q)) - (\sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)) | \\
& + | \sharp\tilde{X}(\mathbb{F}_q) - \sharp\tilde{Y}(\mathbb{F}_q) |
\end{aligned}$$

4. Remarks

4.1. The proof of theorem 4 gives a better upper bound, namely

$$| \sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q) | \leq (\pi_Y - g_Y) - (\pi_X - g_X) + (g_Y - g_X)[2\sqrt{q}].$$

See lemma 4.1 of [3] for the reason of the integer part $[2\sqrt{q}]$ of $2\sqrt{q}$.

4.2. It couldn't be expected theorem 4 to be true for any finite morphism $f : Y \longrightarrow X$. For instance, this is false for the normalization map of a singular curve. Here is another example : let X be the plane curve $Y^2Z = X^3$. This is a singular cubic curve, its arithmetic genus is $\pi_X = 1$, and for any integer n, we have $\sharp X(\mathbb{F}_{2^n}) = 2^n + 1$. Let us consider the morphism

$$\begin{array}{cccc}
\pi : & \mathbb{P}^1 & \longrightarrow & X \\
& (u : v) & \longmapsto & (u^2v : u^3 : v^3)
\end{array}$$

Suppose theorem 4 would be true for any finite morphism f, and let C be any smooth curve of genus g_C, defined over $\mathbb{F}_2$.

There is a finite morphism $\pi' : C \longrightarrow \mathbb{P}^1$, hence by composition a finite morphism $f = \pi \circ \pi' : C \longrightarrow X$, and theorem 4 would imply that for $q = 2^n$,

$$| \sharp C(\mathbb{F}_q) - (q+1) | \leq 2(g_C - 1)\sqrt{q},$$

which is false : one can consider for instance the smooth curve C given by $X^3 + Y^3 + Z^3 = 0$, which has 9 rational points over $\mathbb{F}_4$ and genus $g_C = 1$.

4.3. If X is smooth (in particular if X is the projective line), then any finite morphism $Y \longrightarrow X$ is flat. Indeed, if $f(Q) = P$, then the local ring $\mathcal{O}_{Y,Q}$ is a finitely generated $\mathcal{O}_{X,P}$-module without torsion element. But $\mathcal{O}_{X,P}$ is a principal ideal domain since X is supposed to be smooth, so that $\mathcal{O}_{Y,Q}$ is a flat $\mathcal{O}_{X,P}$-module. This shows that theorem 4 contains all known results (1) and (2) of the introduction.

Note that there are many other situations where $Y \longrightarrow X$ is flat. This is the case for instance if $X = Y/G$, where G is a finite group of automorphisms of Y (see [4]), or (by stability of flatness by base change) if f is the reduction modulo a prime ideal of a flat morphism between two curves defined over a number field, or (also by base change, see section 5 below) if f is a Kummer, or an Artin-Schreier morphism.

5. Application to exponential sums

Let X be a curve over a finite field $\mathbb{F}_q$ of odd characteristic and $f \in \mathbb{F}_q(X)$ a function on X. When X is smooth, there is an extensive literature on estimations of the character sums $\sum_{P \in X(\mathbb{F}_q)} \left(\frac{f(P)}{q}\right)$, where $\left(\frac{\div}{q}\right)$ is the Legendre symbol on $\mathbb{F}_q$ (with the convention that $\left(\frac{f(P)}{q}\right) = 0$ if P is a zero or a pole of f). In fact, this character sum equals to $\sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)$, where Y is the Zariski closure of the curve $\{(P, y) \in X \times \mathbb{P}^1 \mid y^2 = f(P)\}$ in the surface $X \times \mathbb{P}^1$. Indeed, there are exactly $1 + \left(\frac{f(P)}{q}\right)$ points in $Y(\mathbb{F}_q)$ above a given point $P \in X(\mathbb{F}_q)$.

The geometric genus g_Y of Y is given from g_X by Hurwitz formula, and its arithmetic genus is given by the following lemma, whose proof is a standard and tedious calculation using Čech cohomology.

Lemma 6. *Let Y be the Zariski closure of $\{(P, y) \in X \times \mathbb{P}^1 \mid y^n = f(P)\}$. Then, $\pi_Y = n\pi_X + (n-1)(deg(f)_0 - 1)$, where $(f)_0$ denotes the divisors of zeroes of f.*

Since the squaring map $\mathbb{P}^1 \longrightarrow \mathbb{P}^1$, $y \longmapsto y^2$ is flat, then by base change $Y = X \times_{\mathbb{P}^1} \mathbb{P}^1 \longrightarrow X$ is also flat. Hence, theorem 4 applies, so that the following holds :

Theorem 7.

$$\Big| \sum_{P \in X(\mathbb{F}_q)} \left(\frac{f(P)}{q}\right) \Big| \leq 2(n-1)(\pi_X + deg(f)_0 - 1)\sqrt{q}.$$

Of course, one can give a better upper bound using remark 4.1., and one can study additive character sums via Artin-Schreier coverings.

References

[1] Aubry Y., Perret M. : A Weil theorem for singular curves, Proceedings of Arithmetic, Geometry and Coding Theory IV, ed. Pellikaan, Perret, Vlăduţ. De Gruyter, (1995)

[2] Lachaud G. : Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, C. R. Acad. Sci. Paris **305**, 729-732 (1987)

[3] Lachaud G. : Artin-Schreier curves, exponential sums and the Carlitz-Uchiyama bound for geometric codes, J. Number Theory **39**, 18-40 (1991)

[4] Mumford D. : Abelian varieties, Oxford Univ. Press, Oxford 1970

[5] Serre J.-P. : Sur le nombre de points rationnels d'une courbe algébrique sur un corps fini, C. R. Acad. Sci. Paris **296**, série I, 397-402 (1983)

[6] Weil A. : Sur les courbes algébriques et les variétés qui s'en déduisent, Hermann, Paris 1948