ENRICO BOMBIERI

Counting points on curves over finite fields

Séminaire N. Bourbaki, 1974, exp. nº 430, p. 234-241
<http://www.numdam.org/item?id=SB_1972-1973__15__234_0>

COUNTING POINTS ON CURVES OVER FINITE FIELDS

[d'après S. A. STEPANOV]

by Enrico BOMBIERI

I. Let C/k , $k = \mathbb{F}_q$, be a projective non-singular curve of genus g , over a finite field k of characteristic p , with q elements. Let $k_r = \mathbb{F}_{q^r}$ and let $\nu_r(C)$ be the number of k_r-rational points of the curve C . It is well-known that

$$(1) \qquad \nu_r(C) = q^r - \sum_1^{2g} \omega_i^r + 1$$

where the ω_i are algebraic integers independent of r , such that

$$(2) \qquad \omega_i \, \omega_{2g-i} = q \qquad \text{(functional equation)}$$

$$(3) \qquad |\omega_i| = q^{\frac{1}{2}} \qquad \text{(Riemann hypothesis).}$$

Of these results, (1) and (2) are easy consequences of the Riemann-Roch theorem on C , while (3) lies deeper. The first general proof of (3) was obtained by Weil [3], as a consequence of the inequality

$$(4) \qquad |\nu_r(C) - (q^r + 1)| \leq 2g\, q^{r/2} .$$

Until recently, all existing proofs of (3) followed Weil's method, either using the Jacobian variety of C or the Riemann-Roch theorem on $C \times C$. In this talk I want to explain a new approach to (3) invented by S. A. Stepanov [2]. Stepanov himself proved (3) in special cases, e. g. if C was a Kummer or on Artin-Schreier covering of $\mathbb{P}^1$, and a proof in the general case has been also obtained by W. Schmidt. The case in which $g = 2$ has been investigated carefully by

Stark [1], who showed that in certain cases (e. g. $q = 13$) one can get bounds for $\nu_r(C)$ slightly better than those obtainable by (4).

Stepanov's idea is quite simple. One looks for a rational function f on C , not identically 0 , such that

(i) f vanishes at every k-rational point of C , of order $\geq m$, except possibly at a fixed set of m_o rational points of C .

It is now clear that

$$m(\nu_1(C) - m_o) \leq \#\text{ zeros of } f = \#\text{ poles of } f$$

therefore

$$\nu_1(C) \leq m_o + \frac{1}{m}(\#\text{ poles of } f) .$$

If we are able to construct f with not too many poles, then we may get an useful bound for $\nu_1(C)$, essentially of the same strength as (4).

The construction of f given by Stepanov, and also by Schmidt in the general case, is complicated, and in order to prove that f vanishes of order $\geq m$ they consider derivatives or hyperderivatives of f , of order up to $m - 1$. In the final choice, m is about $q^{\frac{1}{2}}$. The argument I will give here, though based on the same idea, does not use derivations and is extremely simple.

II. As Serre pointed out to me, it is more convenient to give C over the algebraic closure $\bar{k}$ of k , to give a Frobenius morphism

$$\varphi : C \to C$$

of order q , and ask for

$$\nu_r = \#\text{ fixed points of } \varphi^r .$$

We begin with

THEOREM 1.- <u>Assume</u> $q = p^{\alpha}$, <u>where</u> α <u>is even</u>. <u>Then if</u> $q > (g+1)^4$ <u>we have</u>

(5) $$\nu_1 < q + (2g+1)q^{\frac{1}{2}} + 1 .$$

For the proof, we may assume that φ has a fixed point x_o , otherwise there is nothing to prove. Now define

R_m = vector space of rational functions on $C/\bar{k}$, such that $(f) \geq - mx_o$.

The following facts are either obvious or trivial consequences of the Riemann-Roch theorem on C .

(i) $\dim R_m \leq m + 1$

(ii) $\dim R_m \geq m + 1 - g$,

with equality if $m > 2g - 2$

(iii) $\dim R_{m+1} \leq \dim R_m + 1$.

Next, we note that since $\varphi(x_o) = x_o$, we have

(iv) $R_m \circ \varphi \subseteq R_{mq}$,

(v) every element $f \circ \varphi$ of $R_m \circ \varphi$ is a q-th power, and we have

$$(f \circ \varphi) = q\varphi((f)) .$$

If A , B are vector subspaces of R_m , R_n we denote by AB the vector subspace of R_{m+n} generated by elements fh , $f \in A$, $h \in B$; also we denote by $R_\ell^{(p^\mu)}$ the subspace of $R_{\ell p^\mu}$ consisting of functions f^{p^μ}, $f \in R_\ell$. Note that

(vi) $$\dim R_\ell^{(p^\mu)} = \dim R_\ell , \qquad \dim R_m \circ \varphi = \dim R_m .$$

The following simple result is the key lemma in the proof.

<u>Lemma</u>.- <u>If</u> $\ell p^\mu < q$, <u>the natural homomorphism</u>

$$R_\ell^{(p^\mu)} \otimes_{\bar{k}} (R_m \circ \varphi) \rightarrow R_\ell^{(p^\mu)}(R_m \circ \varphi)$$

is an isomorphism.

COROLLARY.- If $\ell p^{\mu} < q$ then

(6) $$\dim R_{\ell}^{(p^{\mu})}(R_m \circ \varphi) = (\dim R_{\ell})(\dim R_m) .$$

Proof of Corollary. Obvious from (vi).

Proof of Lemma. Let ord f denote the order of a function f at x_o , so that

$$\text{ord } f \geq -m \qquad \text{for } f \in R_m .$$

By (iii), there is a basis $s_1 , s_2 , \ldots , s_r$ of R_m such that

$$\text{ord } s_i < \text{ord } s_{i+1} \qquad \text{for } i = 1 , 2 , \ldots , r-1 .$$

Now in order to prove the Lemma we have to show that if $\sigma_i \in R_{\ell}$ and if

$$\sum_{i=1}^{r} \sigma_i^{p^{\mu}} (s_i \circ \varphi) \equiv 0$$

then the σ_i are also identically 0 . But assume

$$\sum_{i=\rho}^{r} \sigma_i^{p^{\mu}} (s_i \circ \varphi) \equiv 0 , \quad \sigma_{\rho} \not\equiv 0 .$$

We find

$$\begin{aligned} \text{ord}(\sigma_{\rho}^{p^{\mu}} (s_{\rho} \circ \varphi)) &= \text{ord}(- \sum_{\rho+1}^{r} \sigma_i^{p^{\mu}} (s_i \circ \varphi)) \\ &\geq \min_{i > \rho} \text{ord}(\sigma_i^{p^{\mu}} (s_i \circ \varphi)) \\ &\geq -\ell p^{\mu} + q \ \text{ord } s_{\rho+1} \end{aligned}$$

because $\text{ord}(\sigma_i^{p^{\mu}}) = p^{\mu} \text{ ord}(\sigma_i) \geq -\ell p^{\mu}$ and $\text{ord}(s_i \circ \varphi) = q \text{ ord}(s_i)$, while $\text{ord}(s_i)$ is strictly increasing with i , by our choice of the basis of R_m .

Hence

$$\begin{aligned} p^{\mu} \text{ ord } \sigma_{\rho} &\geq -\ell p^{\mu} + q \ (\text{ord } s_{\rho+1} - \text{ord } s_{\rho}) \\ &\geq -\ell p^{\mu} + q > 0 \end{aligned}$$

and σ_ρ vanishes at x_o . But $\sigma_\rho \in R_\ell$, hence σ_ρ has no poles outside x_o . Hence σ_ρ has no poles and at least one zero, hence $\sigma_\rho \equiv 0$, a contradiction.

Q.E.D.

Proof of Theorem 1. Assume $\ell p^\mu < q$. By the lemma, the map

$$\Sigma\, \sigma_i^{p^\mu}(s_i \circ \varphi) \;\longmapsto\; \Sigma\, \sigma_i^{p^\mu} s_i$$

is well-defined and gives a homomorphism

$$\delta : R_\ell^{(p^\mu)}(R_m \circ \varphi) \to R_\ell^{(p^\mu)} R_m \subseteq R_{\ell p^\mu + m} .$$

By the Corollary of the lemma and by the Riemann-Roch theorem we have

$$\begin{aligned} \dim \ker(\delta) &\geq (\dim R_\ell)(\dim R_m) - \dim R_{\ell p^\mu + m} \\ &\geq (\ell + 1 - g)(m + 1 - g) - (\ell p^\mu + m + 1 - g) \end{aligned}$$

if $\ell , m \geq g$.

Every element $f \in \ker(\delta)$ vanishes of order $\geq p^\mu$ at every fixed point of φ , except possibly at x_o . In fact, if

$$f = \Sigma\, \sigma_i^{p^\mu}(s_i \circ \varphi) \not\equiv 0$$

we have

$$\begin{aligned} f(x) &= \Sigma\, \sigma_i^{p^\mu}(x)\; s_i(\varphi(x)) \\ &= \Sigma\, \sigma_i^{p^\mu}(x)\; s_i(x) \\ &= (\delta f)(x) = 0 , \end{aligned}$$

hence f vanishes at every fixed point of φ , except at x_o . But since every element in $R_\ell^{(p^\mu)}(R_m \circ \varphi)$ is a p^μ-th power, f is a p^μ-th power.

We conclude that f has at least

$$p^\mu(\nu_1 - 1) \text{ zeros.}$$

But $f \in R_\ell^{(p^\mu)}(R_m \circ \varphi) \subseteq R_{\ell p^\mu + mq}$, hence f has at most

$\ell p^{\mu} + mq$ poles.

We conclude that if

$$\ell p^{\mu} < q \quad , \quad \ell \, , m \geq g \quad , \quad \dim \ker(\delta) > 0 \; ,$$

i.e. if

$$(\ell + 1 - g)(m + 1 - g) > \ell p^{\mu} + m + 1 - g$$

then

$$\nu_1 \leq \ell + mq/p^{\mu} + 1 \; . \tag{7}$$

If $q = p^{\alpha}$, α even , $q > (g+1)^4$ we may choose

$$\mu = \alpha/2 \quad , \quad m = p^{\mu} + 2g \quad , \quad \ell = \left[\frac{g}{g+1} p^{\mu} \right] + g + 1$$

and we get the conclusion of Theorem 1.

Q.E.D.

III. The argument given before does not give a lower bound for ν_1 , while this is needed if we want to deduce the Riemann hypothesis (3). For example, if $\nu_r = q^r - \omega_1^r - \omega_2^r + 1$

and $\omega_1 = q$, $\omega_2 = 1$ then (2) is verified, ν_r is always 0 but (3) is false.

For the Riemann hypothesis, we note that we may assume that q is an even power of p , by making a base field extension for C . Also, by a well-known approximation argument, it is sufficient to prove

$$\nu_1 = q + O(q^{\frac{1}{2}}) \; .$$

To prove this, we argue as follows.

The function field $\bar{k}(C)$ of the curve $C/\bar{k}$ contains a purely transcendental subfield $\bar{k}(t)$ such that $\bar{k}(C)$ is a separable extension of $\bar{k}(t)$. Hence there is a normal extension of $\bar{k}(t)$ which is also normal over $\bar{k}(C)$; geometrically, we have a situation

$$C' \to C \to \mathbb{P}^1$$

where $C' \to \mathbb{P}^1$ is Galois, with Galois group G, and $C' \to C$ is also a Galois covering, corresponding to a subgroup H of G. We may assume that G acts on C' over k, by making a finite base field extension. If x is a point of $\mathbb{P}^1$ rational over k and unramified in $C' \to \mathbb{P}^1$, and if y is a point of C' lying over x, we have

$$\varphi(y) = \eta . y$$

for some $\eta \in G$, called the Frobenius substitution of G at the point y. Let $\nu_1(C', \eta)$ be the number of such points of C' with Frobenius substitution η. Arguing as before, but using

$$\delta_\eta : R_\ell^{(p^\mu)}(R_m \circ \varphi) \to R_\ell^{(p^\mu)}(R_m \circ \eta)$$

instead of δ, we obtain easily

(8) $$\nu_1(C',\eta) \le q + (2g' + 1)q^{\frac{1}{2}} + 1 ,$$

where g' = genus of C'. On the other hand

(9) $$\sum_{\eta \in G} \nu_1(C',\eta) = |G|\nu_1(\mathbb{P}^1) + O(1)$$

(the $O(1)$ takes care of the branch points of $C' \to \mathbb{P}^1$). Since

$$\nu_1(\mathbb{P}^1) = q + 1 ,$$

comparison of (8) and (9) gives

(10) $$\nu_1(C',\eta) = q + O(q^{\frac{1}{2}})$$

for every $\eta \in G$. We have also

$$\sum_{\eta \in H} \nu_1(C',\eta) = |H|\nu_1(C) + O(1)$$

whence by (10) we get

$$\nu_1(C) = q + O(q^{\frac{1}{2}}) ,$$

Q.E.D.

REFERENCES

[1] H. STARK - On the Riemann hypothesis in hyperelliptic function fields, to appear.

[2] S. A. STEPANOV - On the number of points of a hyperelliptic curve over a finite prime field, Izv. Akad. Nauk SSSR, Ser. Mat. 33 (1969) 1103-1114.

[3] A. WEIL - Sur les courbes algébriques et les variétés qui s'en déduisent, Hermann (Paris), 1948.