

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

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

where the  $\omega_i$  are algebraic integers independent of  $r$ , such that

$$(2) \quad \omega_i \omega_{2g+1-i} = q \quad (\text{functional equation})$$

$$(3) \quad |\omega_i| = q^{\frac{1}{2}} \quad (\text{RIEMANN hypothesis})$$

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 [4], as a consequence of the inequality

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

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 [3]. STEPANOV himself proved (3) in special cases, e. g. if  $C$  was a KUMMER or an ARTIN-SCHREIER covering of  $\mathbb{P}^1$ , and a proof in the general case has been also obtained by W. SCHMIDT [1]. The case in which  $g = 2$  has been investigated carefully by STARK [2], 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

$f$  vanishes at every  $k$ -rational point of  $C$ , of order  $\geq m$ , except possibly at a fixed set of  $m_0$  rational points of  $C$ .

It is now clear that

$$m(\nu_1(C) - m_0) \leq \# \text{ zeros of } f = \# \text{ poles of } f$$

therefore

$$\nu_1(C) \leq m_0 + \frac{1}{m}(\# \text{ poles of } f).$$

If we are able to construct  $f$  with not too many poles, then we may get a 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 derivatives 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

$$\varphi : C \longrightarrow C$$

of order  $q$ , and ask for

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

We begin with

**THEOREM 1.** — *Assume  $q = p^\alpha$ , where  $\alpha$  is even. Then if  $q > (g + 1)^4$  we have*

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

For the proof, we may assume that  $\varphi$  has a fixed point  $x_0$ , otherwise there is nothing to prove. Now define

$$R_m = \text{vector space of rational functions on } C/\bar{k}, \text{ such that } (f) \geq -mx_0.$$

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  $\varphi(x_0) = x_0$ , we have

- (iv)  $R_m \circ \varphi \subset R_{mq}$   
 (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 the 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  $f^{p^\mu}, f \in R_\ell$ . Note that

- (vi) 
$$\dim R_\ell^{(p^\mu)} = \dim R_\ell,$$
  

$$\dim R_m \circ \varphi = \dim R_m$$

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

LEMMA. — *If  $\ell p^\mu < q$ , the natural homomorphism*

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

*is an isomorphism.*

COROLLARY. — *If  $\ell p^\mu < q$  then*

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

Proof of Corollary. Obvious from (vi).

Proof of Lemma. Let  $\text{ord } f$  denote the order of a function  $f$  at  $x_0$ , so that

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

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

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

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  $\sigma_i$  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

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

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  $\sigma_\rho$  vanishes at  $x_0$ . But  $\sigma_\rho \in R_\ell$ , hence  $\sigma_\rho$  has no poles outside  $x_0$ . Hence  $\sigma_\rho$  has no poles and at least one zero, hence  $\sigma_\rho \equiv 0$ , a contradiction.  $\square$

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

$$\sum \sigma_i^{p^\mu} (s_i \circ \varphi) \mapsto \sum \sigma_i^{p^\mu} s_i$$

is well-defined and gives a homomorphism

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

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  $\varphi$ , except possibly at  $x_0$ . In fact, if

$$f = \sum \sigma_i^{p^\mu} (s_i \circ \varphi) \neq 0$$

we have

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

hence  $f$  vanishes at every fixed point of  $\varphi$ , except at  $x_0$ . But since every element in  $R_\ell^{(p^\mu)}(R_m \circ \varphi)$  is a  $p^\mu$ -th power,  $f$  is a  $p^\mu$ -th power.

We conclude that  $f$  has at least

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

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

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

We conclude that if

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

i.e. if

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

then

$$(7) \quad \nu_1 \leq \ell + mq/p^\mu + 1.$$

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

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

and we get the conclusion of Theorem 1. □

### III.

The argument given before does not give a lower bound for  $\nu_1$ , 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,  $\nu_r$  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

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

where  $C' \rightarrow \mathbb{P}^1$  is GALOIS, with GALOIS group  $G$ , and  $C' \rightarrow C$  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  $C' \rightarrow \mathbb{P}^1$ , 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  $\eta$ . Arguing as before, but using

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

instead of  $\delta$ , we obtain easily

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

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

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

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

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

comparison of (8) and (9) gives

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

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

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

□

## REFERENCES

- [1] Wolfgang M. Schmidt, *Equations over Finite Fields, An Elementary Approach*, Lecture Notes in Math., vol. 536, Springer, 1976.
- [2] Harold M. Stark, *On the Riemann hypothesis in hyperelliptic function fields*, Proc. Sympos. Pure Math., Analytic Number Theory (Harold G. Diamond, ed.), Vol. 24, 1973, pp. 285–302.
- [3] S. A. Stepanov, *On the number of points of a hyperelliptic curve over a finite prime field*, Izv. Akad. Nauk SSSR **33** (1969), 1103–1114.
- [4] André Weil, *Courbes algébriques et variétés abéliennes*, Hermann, Paris, 1948. réimp. 1971.

Enrico BOMBIERI