On the rationality of zeta functions

M. Larsen*

Let $\mathbb{F}_q$ denote a finite field of characteristic p and $V/\mathbb{F}_q$ a variety. For all $n \in N$, we define $a_n = |V(\mathbb{F}_{q^n})|$ and set

$$\zeta_V(x) = \exp\left(\sum_{n=1}^{\infty} \frac{a_n x^n}{n}\right).$$

It is elementary that $\zeta(x) \in \mathbb{Z}[[x]]$, and it is well known [1] that $\zeta(x) \in \mathbb{Q}(x)$. The purpose of this note is to give a simple and elementary proof that the (mod p) reduction, $\bar{\zeta}(x) \in \mathbb{F}_p[[x]]$, is an element of $\mathbb{F}_p(x)$.

By a standard Noetherian induction argument, we may assume that V is affine. Let

$$V = \mathrm{Spec}(\mathbb{F}_q[x_1, \ldots, x_N]/(f_1, \ldots, f_m)).$$

For any non-empty set $\Sigma \subset \{1, 2, \ldots, m\}$, we write V_Σ for the hypersurface in affine N-space defined by $\prod_{i \in \Sigma} f_i$. By the inclusion-exclusion principle,

$$|V(\mathbb{F}_{q^k})| = -\sum_{\emptyset \neq \Sigma \subset \{1,\ldots,m\}} (-1)^{|\Sigma|} |V_\Sigma(\mathbb{F}_{q^k})|.$$

Therefore,

$$\zeta_V(x) = \prod_{\emptyset \neq \Sigma \subset \{1,\ldots,m\}} \zeta_{V_\Sigma}(x)^{-(-1)^{|\Sigma|}}.$$

We may therefore assume that V is actually of the form $\mathrm{Spec}(\mathbb{F}_q[x_1, \ldots, x_N]/(f))$. Given $P = (t_1, \ldots, t_N) \in \mathbb{F}_{q^k}^N$

$$f(t_1, \ldots, t_N)^{q^k - 1} = \begin{cases} 0 & \text{if } P \in V(\mathbb{F}_{q^k}) \\ 1 & \text{if } P \notin V(\mathbb{F}_{q^k}). \end{cases}$$

Therefore,

$$a_k \equiv -\sum_{t_1 \in \mathbb{F}_{q^k}} \cdots \sum_{t_N \in \mathbb{F}_{q^k}} f(t_1, \ldots, t_N)^{q^k - 1} \pmod{p}. \tag{1}$$

The sum of a monomial is given by the formula

$$\sum_{t_1 \in \mathbb{F}_{q^k}} \cdots \sum_{t_N \in \mathbb{F}_{q^k}} t_1^{a_1} \cdots t_N^{a_N} = \begin{cases} (-1)^N & \text{if } a_1 \equiv \cdots \equiv a_N \equiv 0 \pmod{q^k - 1} \\ 0 & \text{otherwise.} \end{cases}$$

* Supported by N.S.F. Grant No. DMS-8807203

For $I \in \mathbb{N}^N$, we write x^I for the corresponding monomial in $x_1, \ldots, x_n$, and $c_I(g)$ for the x^I coefficient of $g \in \mathbb{F}_q[x_1, \ldots, x_N]$. By (1),

$$a_k \equiv -(-1)^N \sum_I c_{(q^k-1)I}(f^{q^k-1}) \pmod{p}. \tag{2}$$

If S denotes the convex hull of

$$\{I | c_I(f) \neq 0\} \cup \{I | c_I(f^{q-1}) \neq 0\},$$

the sum in (2) can be taken over $T = S \cap \mathbb{N}^n$. Setting $g = f^{q-1}$,

$$f^{q^k-1} = g g^q g^{q^2} \cdots g^{q^{k-1}}.$$

As

$$c_I(g^{q^r}) = \begin{cases} c_{q^{-r}I}(g) & \text{if } q^r | I, \\ 0 & \text{otherwise,} \end{cases}$$

we have

$$c_I(f^{q^k-1}) = \sum_{J_0 + qJ_1 + \cdots + q^{k-1}J_{k-1} = I} c_{J_0}(g) c_{J_1}(g) \cdots c_{J_{k-1}}(g).$$

If

$$J_0 + qJ_1 + \cdots + q^{k-1}J_{k-1} = (q^k - 1)I,$$

there exist unique multi-indices $I_1, \ldots, I_{k-1}$ such that

$$J_i = qI_{i+1} - I_i, \quad i = 0, \ldots, k-1,$$

where $I_0 = I_k = I$. Moreover, if I and all J_i lie in T, so do all I_i. We conclude that

$$a_k \equiv -(-1)^N \sum_{I_0, I_1, \ldots, I_{k-1}} c_{qI_1 - I_0}(g) c_{q^2 I_2 - qI_1}(g) \cdots c_{q^k I_0 - q^{k-1} I_{k-1}}(g) \pmod{p}.$$

If

$$M_{I,J} = c_{qI-J}(g)$$

denotes a square matrix of order $|T|$, then

$$a_k \equiv -(-1)^N tr(M^k) \pmod{p}.$$

The right hand side is the sum of N^{th} powers of the eigenvalues λ_i of M. From this it follows immmediately that

$$\zeta_V(x) = \prod_i (1 - \lambda_i x)^{(-1)^{N+1}}.$$

REFERENCES

[1] B. Dwork, On the rationality of the zeta function of an algebraic variety, *Amer. Jour. Math.*, **82** (1960), 631-648.