Throughout this writeup, let \( V \) be an algebraic set defined over \( \mathbb{F}_q \) where \( q \) is a prime power.

1. Prime Zero-Cycles

Fix an algebraic closure \( \overline{\mathbb{F}}_q \) of \( \mathbb{F}_q \). Once the algebraic closure is fixed, it is the union of the finite extension fields of \( \mathbb{F}_q \),

\[
\overline{\mathbb{F}}_q = \bigcup_{f \geq 1} \mathbb{F}_{q^f}.
\]

Also, the algebraic set \( V \) is the union of its points having coordinates in the finite extensions,

\[
V = \bigcup_{f \geq 1} V(\mathbb{F}_{q^f}).
\]

For each \( f \geq 1 \), the Galois group (automorphism group) of \( \mathbb{F}_{q^f} \) over \( \mathbb{F}_q \) is cyclic of order \( f \), generated by \( x \mapsto x^q \).

**Definition 1.1.** Consider a point \( \alpha \in V \). The **degree** of \( \alpha \) is the smallest \( f \) such that \( \alpha \in V(\mathbb{F}_{q^f}) \). The **prime zero-cycle** (or **prime divisor**) of \( \alpha \) is the orbit of \( \alpha \) under the Galois action,

\[
P_\alpha = \{ \alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{f-1}} \}.
\]

The **degree** of the zero cycle is

\[
\deg(P_\alpha) = f,
\]

and the **norm** of the zero cycle is

\[
N(P_\alpha) = q^f.
\]

2. The Counting Zeta Function

For each \( f \geq 1 \), let

\[
N_f(V) = |V(\mathbb{F}_{q^f})|,
\]

and let \( a_f \) be the number of prime zero-cycles having degree \( f \). Then since \( V(\mathbb{F}_{q^f}) \) is the disjoint union of all prime zero-cycles of all degrees \( d \mid f \),

\[
N_f(V) = \sum_{d \mid f} a_d d.
\]

**Definition 2.1.** The **counting zeta function** of \( V \) is

\[
Z(V, T) = \exp \left( \sum_{f \geq 1} \frac{N_f(V)}{f} T^f \right).
\]
Proposition 2.2. The counting zeta function of an algebraic set has an Euler factorization over prime zero cycles,

$$Z(V, T) = \prod_{\mathfrak{P}} (1 - T^{f(\mathfrak{P})})^{-1}.$$ 

 Especially, 

$$Z(V, q^{-s}) = \prod_{\mathfrak{P}} (1 - N_{\mathfrak{P}}^{-s})^{-1}.$$ 

**Proof.** For any $d \geq 1$, recall that $a_d$ denotes the number of prime zero cycles of degree $d$, all of which have norm $d$. Thus

$$\prod_{\mathfrak{P}} (1 - T^{f(\mathfrak{P})})^{-1} = \prod_{d \geq 1} (1 - T^d)^{-a_d}.$$ 

Take the logarithmic derivative,

$$(\log(\prod_{\mathfrak{P}} (1 - T^{f(\mathfrak{P})})^{-1}))' = \sum_{d \geq 1} \frac{-a_d (1 - T^d)^{-a_d} (-d T^{d-1})}{(1 - T^d)^{-a_d}} = \sum_{d \geq 1} \frac{a_d d T^{d-1}}{1 - T^d}.$$ 

Rearrange the right side, recalling that $\sum_{d | f} a_d = N_f(V)$ at the last step,

$$\sum_{d \geq 1} \frac{a_d d T^{d-1}}{1 - T^d} = \sum_{d \geq 1} a_d d T^{d-1} \sum_{e \geq 0} T^{de} = \frac{1}{T} \sum_{d \geq 1} a_d d \sum_{e \geq 1} T^{de}$$

$$= \frac{1}{T} \sum_{f \geq 1} \left( \sum_{d | f} a_d d \right) T^f = \sum_{f \geq 1} N_f(V) T^{f-1}.$$ 

That is,

$$(\log(\prod_{\mathfrak{P}} (1 - T^{f(\mathfrak{P})})^{-1}))' = \left( \sum_{f \geq 1} \frac{N_f(V)}{f} T^f \right)'.$$ 

Hence (after checking a constant)

$$\log(\prod_{\mathfrak{P}} (1 - T^{f(\mathfrak{P})})^{-1}) = \sum_{f \geq 1} \frac{N_f(V)}{f} T^f = \log(Z(V, T)),$$

and the result follows. 

\[\square\]

3. A Rationality Criterion

Because the counting zeta function takes the form

$$Z(V, T) = 1 + \cdots ,$$

it is rational if and only if it takes the form

$$Z(V, T) = \frac{\prod_{\alpha} (1 - \alpha_i T)}{\prod_{\beta} (1 - \beta_j T)}, \quad \text{all } \alpha_i, \beta_j \in \mathbb{F}_q .$$

**Proposition 3.1.** The counting zeta function of an algebraic set takes the form

$$Z(V, T) = \frac{\prod_{\alpha} (1 - \alpha_i T)}{\prod_{\beta} (1 - \beta_j T)}.$$
if and only if the solution-counts take the form
\[ N_f(V) = \sum_j \beta_f^j - \sum_i \alpha_f^i. \]

**Proof.** Compute that the condition
\[ Z(V, T) = \prod_i (1 - \alpha_i T) \prod_j (1 - \beta_j T) \]
is equivalent to the condition
\[
\log Z(V, T) = \sum_j \log(1 - \beta_j T)^{-1} - \sum_i \log(1 - \alpha_i T)^{-1} \\
= \sum_j \sum_{f \geq 1} \frac{(\beta_j T)^f}{f} - \sum_i \sum_{j \geq 1} \frac{(\alpha_i T)^f}{f} \\
= \sum_{f \geq 1} \frac{\left(\sum_j \beta_f^j - \sum_i \alpha_f^i\right)}{f} T^f
\]
which in turn is equivalent to the condition
\[ N_f = \sum_j \beta_f^j - \sum_i \alpha_f^i. \]

For an elliptic curve over \( \mathbb{F}_p \) where \( p \) is prime, the solution count is
\[ N_f(E) = p^f + 1 - \alpha_1^f - \alpha_2^f \]
where, letting \( a_p(E) = p + 1 - |E(\mathbb{F}_p)|, \)
\[ X^2 - a_p(E)X + p = (X - \alpha_1)(X - \alpha_2). \]
Thus the counting zeta function is
\[ Z_p(E) = \frac{1 - a_p(E)T + pT^2}{(1 - T)(1 - pT)}. \]
The more familiar counting zeta function of \( E \),
\[ \widetilde{Z}_p(E) = (1 - a_p(E)T + pT^2)^{-1}, \]
uses only the normalized solution-count
\[ t_f(E) = p^f + 1 - N_f(E) = \alpha_1^f + \alpha_2^f \]
rather than all of \( N_f(E) \).