- Now, over k', $f(T)$ splits as a product $f(T) = f_1 \cdots f_e$, of equi-degree irreducible polynomials. (Why?)
- Further, $e = \gcd(n, d(P))$. (Exercise)
- This factorization suggests that $P \in C$ corresponds to e points $Q_1, \ldots, Q_e \in C_n$ of equal degree and:

$$d(P) = \sum_{i=1}^{e} d(Q_i) = e \cdot d(Q_1).$$

- Thus, the contribution in $Z(t^n, C_n)$ corresponding to P is: $\prod_{i=1}^{e} \left(1 - t^{n d(P)/e}\right)^{-1}$.

- Claim: $\left(1 - t^{n d(P)/e}\right)^e = \prod_{\eta^n = 1} \left(1 - (\eta t)^{d(P)}\right)$.

Pf: • Let $n' := n/e$ & $d' := d(P)/e$.
- Since, $e = \gcd(n, d(P))$ we have $(n', d') = 1$.
- RHS $= \prod_{\eta} \left(1 - \eta^{ed'} \cdot t^{d(P)}\right)$
- Now, as η runs over $\sqrt[n]{1}$, η^e runs over $\sqrt[n']{1}$.

$\Rightarrow (\eta^e)^{d'}$ runs over $\sqrt[n']{1}$ (with e repetitions).

$\Rightarrow$ RHS $= \left(1 - t^{n' \cdot d(P)}\right)^e =$ LHS. $\square$

• Going back, the contribution of P in $Z(t^n, C_n)$ is: $\prod_\eta (1-(\eta t)^{d(P)})^{-1}$.

$\Rightarrow Z(t^n, C_n) = \prod_\eta Z(\eta t, C)$. $\square$

- Corollary (Two poles) $\delta = 1$.

Pf: • The functional equation calculation tells us: $Z(t,C) = \dfrac{L(t)}{(1-t^\delta)\cdot(1-(qt)^\delta)}$

where $L(t) \in \mathbb{Z}[t]$.

• Fix $n=\delta$ and apply base change:

$$Z(t^\delta, C_\delta) = \prod_{\eta^\delta=1} Z(\eta t, C) = \prod_\eta \frac{L(\eta t)}{(1-t^\delta).(1-(qt)^\delta)}$$

$$= \frac{L(t^\delta)}{(1-t^\delta)^\delta\cdot(1-(qt)^\delta)^\delta}.$$

• From the fact that $Z(t^\delta, C_\delta)$ has simple poles, we deduce $\delta = 1$! $\square$

- Also, note that $L(0) = Z(0) = 1$ and $L(1) = \text{residue of } Z(t) \text{ at } (t=1) = h(C)$.
- We collect these results:

- <u>Theorem:</u> Let C be a smooth proj. curve over $k = \mathbb{F}_q$ with fn. field K; suppose k is the exact field of constants of K. Then,

(i) We have an exact sequence
$$0 \to Cl_0(C) \to Cl(C) \xrightarrow{d(\cdot)} \mathbb{Z} \to 0.$$

(ii)
$$Z(t, C) = \frac{L(t)}{(1-t)(1-qt)},$$
where $L(t) \in \mathbb{Z}[t]$ has degree $2g$, and
$$L(t) = (qt^2)^g \cdot L(1/qt).$$

(iii) $L(0) = 1$ & $L(1) = h(C)$.

Consequences to counting

- Let C be the curve over $k = \mathbb{F}_q$ with zeta fn. $Z(t)$, as before.

- Euler product says $Z(t) = \prod_{P \in C} (1 - t^{d(P)})^{-1}$.

$$\Rightarrow Z'(t) = Z(t) \cdot \sum_{P \in C} \frac{\frac{\partial}{\partial t}(1 - t^{d(P)})^{-1}}{(1 - t^{d(P)})^{-1}}$$

$$\Rightarrow t \cdot \frac{Z'}{Z} = \sum_{P \in C} d(P) \cdot t^{d(P)} \cdot (1 - t^{d(P)})^{-1}$$

$$= \sum_{P \in C} d(P) \cdot \sum_{n \geq 1} t^{n \cdot d(P)}$$

number of $\mathbb{F}_{q^m}$-points in C

$$= \sum_{m \geq 1} t^m \cdot \sum_{d(P) | m} d(P) = \sum_{m \geq 1} N_m \cdot t^m$$

$$\Rightarrow \frac{d}{dt}(\log Z) = \sum_{m \geq 1} N_m \cdot t^{m-1}$$

Integrating, we get:

- **Proposition:** $Z(t, C) = \exp\left(\sum_{m \geq 1} \frac{N_m}{m} \cdot t^m\right)$.

- Since, we know that $Z(t) = \frac{L(t)}{(1-t)(1-qt)}$ & that $L(0) = 1$, we write:

$$Z(t) = \prod_{1 \leq i \leq 2g} (1-\alpha_i t) \Big/ (1-t).(1-qt) \, ,$$

where, α_i^{-1} are the $2g$ roots (in $\mathbb{C}$) of $L(t)$.

$$\Rightarrow \exp\left(\sum_{n \geq 1} \frac{N_n}{n}.t^n\right) = \exp\left\{\sum_{i=1}^{2g} \log(1-\alpha_i t) - \log(1-t) - \log(1-qt)\right\}.$$

- Comparing the two power series, we get:

<u>Proposition</u>: $\forall n \in \mathbb{N}, \quad N_n = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n$.

- <u>Rmk</u>: We view $\sum_{i=1}^{2g} \alpha_i^n$ as the <u>error term</u> in this estimate for N_n. It will be bounded tightly by the <u>Riemann hypothesis</u>.

- Invoking the symmetry: $L(t) = (qt^2)^g \cdot L(1/qt)$, we also get (for some labelling of α's):

<u>Exercise</u>: $\forall i \in [g], \quad \alpha_i \cdot \alpha_{i+g} = q$.