- Thus, we've shown for any smooth proj. curve $C$ over $\mathbb{F}_q$, genus $g$, the roots $\alpha$ of $L(t)$ satisfy $|\alpha| = \sqrt{q}$.
- $$-2g\sqrt{q} \le N_1(C) - (q+1) \le 2g\sqrt{q}.$$

$\Rightarrow$ For $q \gg g^2$, $N_1(C) \approx q+1 = N_1(\mathbb{P}^1)$.

- RH has tons of implications. For eg. in CS we use:

<u>Corollary</u> (Weil estimate for $\chi$-sums): Let $\chi = \chi_2 : \mathbb{F}_q \to \{-1, 0, +1\}$ be the character

$\alpha \mapsto \alpha^{(q-1)/2} = 1$ iff $\alpha$ is square in $\mathbb{F}_q$.

Let $f(x)$ be deg-$\delta$ polynomial. Then,

$$\left| \sum_{\alpha \in \mathbb{F}_q} \chi(f(\alpha)) \right| \leq O_\delta(\sqrt{q}).$$

Pf: • Consider the curve $C$ for $K := \mathbb{F}_q(x)[y]/\langle y^2 - f \rangle$.

• $$\sum_{\alpha \in \mathbb{F}_q} \chi(f(\alpha)) = \sum_{\alpha : \chi(f(\alpha)) = 1} 1 - \sum_{\alpha : \chi(f(\alpha)) = -1} 1$$

$$= \sum_{\alpha : \chi(f(\alpha)) = 1} 2 - \sum_{\alpha : \chi(f(\alpha)) = -1, 1} 1 = N_1(C) - q + O_\delta(1).$$

$$= O_\delta(\sqrt{q}). \qquad \square$$

Exercise: Do this for other exponential sums.

Qn: (i) Given $C/\mathbb{F}_q$, how do we compute $N_1(C)$ in $\mathrm{poly}(\lg q)$-time?

(ii) Is there another interpretation of $L(t)$ that can help in computing?

# Cohomological interpretation of $L(t)$

- See Frob ($q$-th) $\pi$ as an isogeny on Jacobian.
- Defn: • Isogeny $\alpha : J_C(\bar{k}) \to J_C(\bar{k})$ is a surjective morphism with finite $\ker(\alpha)$.
  (respecting the group & the variety)
  • $\deg(\alpha) := |\ker(\alpha)|$.

- Eg. 1. $\pi : J \to J$ is an isogeny with $\deg(\pi) = 1$.
- Eg. 2. For $n \in \mathbb{Z}$, $[n] : J \to J$ ; $D \mapsto n \cdot D$ is an isogeny. What's $\deg([n]) = ?$

- Defn: • For prime $\ell \in \mathbb{N}$, we call $\ker([\ell])$ the <u>$\ell$-torsion of $J$</u>, denoted $J[\ell]$.

• $\underline{T_\ell J} := \bigcup_{i \geq 1} J[\ell^i]$ is <u>$\ell$-adic torsion of $J$</u>.

• Any isogeny $\alpha : J \to J$ gives an isogeny $\underline{T_\ell \alpha} : T_\ell J \to T_\ell J$ ; $D \mapsto \alpha(D)$.

- Now, we can study $T_\ell \alpha$ for $\alpha$ coming from $T_l$ & $[n]$.

<u>Theorem (Weil):</u> (a) Linear map $\pi$ on $T_\ell J$ has charpoly $t^{2g} \cdot L(1/t)$. (Assume $\ell \neq p$.)

(b) $T_\ell J \cong (\mathbb{Z}_\ell)^{2g}$, i.e. $T_\ell J$ is a finite rank $\mathbb{Z}_\ell$-module.

(c) For any $n \in \mathbb{N}$, $\deg([n]) = n^{2g}$ & $J[n] \cong (\mathbb{Z}/n)^{2g}$.

Pf: Recall, $\deg(\pi - 1) = |J(k)| = |Cl_0(C)| = h(C)$
$$= L(1) = \prod_{i \in [2g]} (\alpha_i - 1).$$

- Similarly, $\forall m \in \mathbb{N}$, $\deg(\pi^m - 1) = |J(\mathbb{F}_{q^m})|$
$$= \prod_i (\alpha_i^m - 1)$$
[Base-change of $L(t)$]

- Going to $\mathbb{Z}_\ell$, we can view $\alpha_i$ in $\mathbb{C} \cap \overline{\mathbb{Q}_\ell}$.

- Let $\pi$ act on $T_\ell J$ with eigenvalues $\beta_i$, $i \in \mathbb{N}$.

$$\Rightarrow \deg(\pi^m - 1) = |T_\ell J / (\pi^m - 1) T_\ell J| = \det(T_\ell(\pi^m - 1))$$

(|ker| = |coker| = det = $\prod$ eigenval)

$$= \prod_i (\beta_i^m - 1).$$

- Since, this holds $\forall m$, we deduce that $\alpha_i$'s = $\beta_i$'s = eigenvals of $T_\ell \pi$ $\Rightarrow$

$\triangleright$ $\mathrm{charpoly}(\pi | T_\ell J) = t^{2g} \cdot L(1/t)$ over $\mathbb{Z}_\ell$.

- Also, $\rhd$ charpoly $(\pi^{-1}|_{T_\ell J}) = q^{-g} \cdot L(t)$, over $\mathbb{Z}_\ell$.

- (b) & (c) are implied by $\deg L = 2g$ & $\ell^i$-torsion resp. $n$-torsion of $J$.

$\square$

→ These properties are computationally useful, as one can try computing $L(t)$ mod $\ell$ ! (or compute $p$-adically.)

- Current time-complexity for $L(t)$ is the min of: $\mathrm{poly}(p, g, \delta)$ [Kedlaya, 2001] and $\mathrm{poly}(\lg p, 2^{2^g}, \delta)$ [Pila, 1990].