Computing the Zeta function

- The tools we developed till now are not yet enough to actually compute $Z(t,C)$.

- The key idea, due to Weil, that we now study is: The Frobenius map F acts linearly on the Jacobian variety $J(C)$, or $Cl_0(C)$, and its characteristic polynomial is $Z(t,C)$!

- To get an algorithm out of this we need the addition algorithm on $J(C)$. This we sketch only for the curve C: $y^2 = f(x)$, called a hyperelliptic curve.

- The details we skip could be found in standard articles.

Frobenius interpretation of $Z(t,c)$

- Recall that $Z(t,c) = \dfrac{L(t)}{(1-t)(1-qt)}$,
where, $\deg L = 2g$, $L(0) = 1$, and L is an integral polynomial.

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

- We want to interpret N_m as fixed pts. of the Frobenius map $F: \overline{C} \to \overline{C}$, where $\overline{C}$ is the curve C over $\overline{k} = \overline{\mathbb{F}_q}$.
- In this case F maps an actual point $P = (a_i)$ to $F(P) = (a_i^{q'})$.

- So, $N_m(C) = N_m(\overline{C})$ can be viewed as the $\#\{$fixed pts. of F^m on $\overline{C}\}$.

- Now let us consider the action of F on $Cl_0(\overline{C})$.

- We denote the m-th linear map as $(F^m; J(\bar{C}))$.

- Since J is finite, we have for any prime ℓ, the ℓ-torsion points $J[\ell] \subset J$ are finite.
(I.e. $D \in J$ s.t. $\ell \cdot D = 0$.)

- Thus, $J[\ell]$ is a finite dimensional vector space over $\mathbb{F}_\ell$.

- It can be shown that, for prime $\ell \neq p$, F is a $\mathbb{F}_\ell$-linear automorphism of $J[\ell]$.

- Using these ideas, Weil gave a second proof of the RH via ℓ-adic means!

- In particular, he showed that:

$$L(t, C) \equiv \det(1 - Ft; J[\ell]) \pmod{\ell}.$$

▷ I.e. $L(t)$ is the characteristic polynomial of the Frobenius map on $J[\ell]$.

Sketch:

- Weil gave three $\mathbb{Q}_\ell$-vector spaces $H^i(C)$, $(i=0,1,2)$ s.t. $N_m(C) = \#\{\text{fixed pts. of } F^m \text{ on } \bar{C}\}$
$$= \sum_{i=0}^{2} (-1)^i \cdot \mathrm{Tr}(F^m; H^i(C))$$

$$\Rightarrow Z(t,C) = \exp\Big(\sum_{\substack{0\le i\le 2\\ m\geq 1}} (-1)^i \mathrm{Tr}(F^m; H^i(C)) \frac{t^m}{m}\Big)$$
$$= \prod_{i=0}^{2} \Big\{\exp\Big(\sum_{m\geq 1} \mathrm{Tr}(F^m; H^i(C)) \frac{t^m}{m}\Big)\Big\}^{(-1)^i}$$

- This can be simplified!
- Claim: If φ is an endomorphism of a finite dim. vector space V over $\mathbb{F}$, then
$$\exp\Big(\sum_{m\geq 1} \mathrm{Tr}(\varphi^m; V) \cdot \frac{t^m}{m}\Big) = \big(\det(1-\varphi t; V)\big)^{-1}.$$

Pf: • Let $\dim V = 1$. Then, $\exists \lambda \in \mathbb{F}$ s.t. $\varphi: v \mapsto \lambda v$, $\forall v \in V$.

• In this case, $LHS = \exp\Big(\sum_{m\geq 1} \frac{\lambda^m t^m}{m}\Big)$
$$= \exp(-\log(1-\lambda t)) = (1-\lambda t)^{-1} = RHS.$$

• If $\dim V > 1$, do induction on $\dim V$; by picking a

φ-invariant subspace $V' \subset V$.

- So, LHS $= \exp\left(\sum_{m\geq 0} Tr(\varphi^m; V') \frac{t^m}{m}\right)$.

$$\exp\left(\sum_{m\geq 0} Tr(\varphi^m; V/V') \frac{t^m}{m}\right)$$

$$= \det(1-\varphi t; V')^{-1} \cdot \det(1-\varphi t; V/V')^{-1}$$
$$= \det(1-\varphi t; V)^{-1} = \text{RHS}. \qquad \square$$

- Thus, $Z(t,C) = \dfrac{\det(1-Ft; H^1(C))}{\det(1-Ft; H^0(C)) \cdot \det(1-Ft; H^2(C))}$

- It turns out that:
  $L(t,C) = \det(1-Ft; H^1(C))$,
  the other two give $(1-t)\cdot(1-qt)$, &
  $H^1(C) \pmod{\ell}$ is exactly $J[\ell]$.
- This is called the cohomological interpretation of the zeta fn.
- Weil conjectured this pattern also for the general varieties!

- Since the coefficients of $L(t)$, by RH, are of magnitude $\leqslant \binom{2g}{g}(\sqrt{q})^{2g}$; it will suffice in Chinese remaindering to compute $L(t) \pmod{\ell}$ for the first $\log\left(2\cdot\binom{2g}{g}q^{g}\right) = (\log q)^{O(g)}$ many primes.

- Adleman-Huang (2001) gave an algorithm to do this in time $(\log q)^{O(g^2 \log g)}$, assuming that:

  C is a <u>hyperelliptic curve</u>, i.e. the fn. field $K = \mathbb{F}_q(x)[y]/\langle y^2 - f(x)\rangle$.

- For general curves C we may not even be able to compute within $J(C)[\ell]$.