The Riemann Hypothesis

- We intend to show: $\forall i \in [2g], |\alpha_i| = \sqrt{q}$.

- In terms of $\zeta(s, C) = Z(q^{-s}, C)$, it means that the zeros of ζ are on the line $Re(s) = 1/2$. ← RH

- The number theory importance of this result is: $|N_n - (q^n+1)| = \left|\sum_{i=1}^{2g} \alpha_i^n\right| \leq 2g \cdot q^{n/2}$.

- Thus, # $\mathbb{F}_q$-points on a curve are in the range $[q+1-2g\sqrt{q}, q+1+2g\sqrt{q}]$.

- Proposition: RH is true for $Z(t, C)$ iff it is so for $Z(t, C_n)$.

Pf: • We have $Z(t^n, C_n) = \prod_{\eta^n=1} Z(\eta t, C)$.

• Further, use $(1-\alpha^n t^n) = \prod_{\eta^n=1} (1-\alpha\eta t)\cdot(-1)^{n-1}$. □

- <u>Proposition</u>: TFAE:

(i) RH holds for $Z(t, C)$.

(ii) $\exists$ constants $A, B, N \in \mathbb{N}$ s.t. $\forall$ <u>large</u> multiples d of N: $|N_d - (q^d+1)| \leq A + Bq^{d/2}$.

- <u>Proof</u>: • (i) $\Rightarrow$ (ii): As seen before, the reason is the error-term $\sum_{i=1}^{2g} \alpha_i^d$.

• (ii) $\Rightarrow$ (i): We replace the base field $\mathbb{F}_q$ by $\mathbb{F}_{q^N}$. Thus, the hypothesis implies:

$$\Big|\sum_{1\leq i\leq 2g} \alpha_i^d\Big| = |N_d - (q^d+1)| \leq A + Bq^{d/2}$$

for all $d \in \mathbb{N}$.

• Since $\prod \alpha_i = q^g$, it suffices to show $|\alpha_i| \leq \sqrt{q}, \forall i$.

• Recall $L(t) = \prod_{1\leq i\leq 2g} (1-\alpha_i t)$, so

$$-\log L(t) = \sum_{d\geq 1} \left(\sum_{i=1}^{2g} \alpha_i^d t^d / d \right)$$

$$\Rightarrow \left|\log \frac{1}{L}\right| \leq \sum_{d\geq 1} (A + Bq^{d/2}) \frac{|t|^d}{d}$$

$$\leq A \cdot \log(1-|t|)^{-1} + B \cdot \log(1-|t\sqrt{q}|)^{-1}$$

$\Rightarrow$ The power series converges (absolutely) for any $t \in \mathbb{C}$ with $|t| < q^{-1/2}$.

$\Rightarrow$ All the poles of $\log \frac{1}{L(t)}$ lie in the region $|t| \geq q^{-1/2}$.

$\Rightarrow$ The zeros of $L(t)$ have to satisfy:

$\forall i,\ |\alpha_i^{-1}| \geq q^{-1/2}$

$\Rightarrow\ \forall i \in [2g],\ |\alpha_i| \leq \sqrt{q}$. $\square$

Move to the Galois covering

- e.g. Let C be a smooth projective curve over $k = \mathbb{F}_q$. In the affine patch $x_0 = 1$, let it be given by: $x_2^3 = x_2 + x_1^2$.

$\Rightarrow K(C) =: K = k(x_1)[x_2] / \langle x_2^3 - x_2 - x_1^2 \rangle$.

- We see that K is a finite extn. of $k(x_1)$, but is not Galois (i.e. not all the roots of $x_2^3 - x_2 - x_1^2 = 0$ are in K).