— Secondly, if $Q \neq P$ is a point in C s.t. $F(Q) = \sigma(Q)$ $[\Rightarrow \varphi(Q) = Q]$, then $G|_Q = \left(\sum_i (s_i F^{\mu}_{abs}) \cdot (f_i \circ \varphi)\right)\Big|_Q = \left(\sum_i (s_i F^{\mu}_{abs}) \cdot f_i\right)\Big|_Q = 0.$

P may be a pole of G

$\Rightarrow$ Q is a zero of G

— Overall, we deduce:

$$p^{\mu} \cdot (N_1(C,\sigma) - 1) \leq d((G)_0) = d((G)_\infty) \leq bp^{\mu} + aq.$$

$$\Rightarrow N_1(C,\sigma) \leq b + 1 + aqp^{-\mu}.$$

— Thus, to finish the theorem we just need:

<u>Claim 2:</u> If we take $\mu = \alpha/2$, $a = \sqrt{q} + 2g$ & $b = g + 1 + \lfloor g\sqrt{q}/(g+1) \rfloor$, then,

(i) $bp^{\mu} < q$

(ii) $\ell_b \ell_a > \ell_{bp^{\mu}+a}$

(iii) $b + 1 + aqp^{-\mu} < q + 1 + (2g+1)\sqrt{q}$.

It'll help to take $b \approx p^{\mu}$ in (i); that gives the error-term $\sqrt{q}$!

<u>Proof:</u> • We have $p^{\mu} = p^{\alpha/2} = \sqrt{q}$.

• Also, $q > (g+1)^4$ gives:

$$\sqrt{q}/(g+1) - g - 1 > 0.$$

(i) $b = g+1+\lfloor g\sqrt{q}/(g+1)\rfloor + \sqrt{q}/(g+1) - \sqrt{q}/(g+1)$

$$\leq p^{\mu} + g+1 - \sqrt{q}/(g+1)$$
$$< p^{\mu} = \sqrt{q}.$$
$$\Rightarrow \quad bp^{\mu} < q.$$

(ii) $\because$ $b, a \geqslant 2g$, Riemann-Roch implies that we just need to verify:

$$(b+1-g)(a+1-g) > (bp^{\mu}+a+1-g)$$

iff $(b-g)(a+1-g) > bp^{\mu}$

iff $b(a+1-g-p^{\mu}) > g(a+1-g)$

iff $b(1+g) \qquad > g(1+g+\sqrt{q})$

iff $\qquad b \quad > g\left(1+\frac{\sqrt{q}}{g+1}\right)$, which is true!

(iii) $b + aqp^{-\mu} + 1 = g+1+ \lfloor g\sqrt{q}/(g+1) \rfloor + (2g+\sqrt{q})\sqrt{q} + 1$

$$\leq g+1+\frac{g\sqrt{q}}{g+1} + 2g\sqrt{q} + q + 1$$

$$= 1+q+(2g+1)\sqrt{q} - \left(\frac{\sqrt{q}}{g+1} - g - 1\right)$$

$$< 1+q+(2g+1)\sqrt{q}.$$

$\square$ (Pf-Claim-2)

$\square$ (Pf-Theorem)

– This finishes the Riemann Hypothesis:

For any smooth proj. curve C over $\mathbb{F}_q$, with genus g, the roots α of $Z(t,C)$ satisfy $|\alpha| = \sqrt{q}$.

Equivalently, the number of $\mathbb{F}_q$-points on C is: $q+1-2g\sqrt{q} \leq \underset{\left(q+1-\sum_{i=1}^{2g}\alpha_i\right)}{\overset{\shortparallel}{N_1(C)}} \leq q+1+2g\sqrt{q}$.

Thus, when $q \gg g$, there are around q rational points on any proj. curve!