§11 Proof of the Riemann Hypothesis for curves over finite fields

We fix for the moment $k = \bar{k}$ alg closed field

C_1, C_2 smooth proj integral curves $/k$

set $X := C_1 \times C_2$

This is a smooth proj integral surface

Fix $x_i \in C_i(k)$ $\quad (k = \bar{k} \,!)$

set $F_1 := C_1 \times \{x_2\}$, $F_2 := \{x_1\} \times C_2$

$\Rightarrow F_1, F_2 \subset X$ smooth curves.

① **Lemma:** Situation as above

Then.

(i) $(F_1 \cdot F_2) = 1$

(ii) $(F_1 \cdot F_1) = (F_2 \cdot F_2) = 0$

(iii) $A := F_1 + F_2$ is an ample divisor on X

Pf: (i) F_1 and F_2 intersect properly

$$\Rightarrow (F_1 \cdot F_2) = \sum_{x \in F_1 \cap F_2} i_x(F_1, F_2)$$

$$F_1 \cap F_2 = \{x_1 \times x_2\} \qquad A_i = \mathcal{O}_{C_i, x_i} \ni t_i \text{ loc param.}$$

$$\updownarrow$$

$$P \subset A_1 \otimes A_2$$

$$\Rightarrow \qquad \mathcal{O}_{X, x_1 \times x_2} = (A_1 \otimes A_2)_P$$

$$\left.\begin{array}{lll} \text{eq for } & F_2 & = t_1 \otimes 1 \\ & F_1 & = 1 \otimes t_2 \end{array}\right\} \to \text{gen max'l ideal}$$

$$\Rightarrow (F_1 \cdot F_2) = \ell\left(\frac{(A_1 \otimes A_2)_P}{(t_1 \otimes 1, 1 \otimes t_2)}\right) = 1 \qquad \Rightarrow \text{i)}$$

(ii) $RR \Rightarrow \exists \; f \in H^0(C_1, \mathcal{O}_{C_1}(nx_1)) \setminus k$

some $n \gg 0$.

$\Rightarrow \quad \operatorname{div} f = -r x_1 + \alpha$

$n \geq r \geq 1 \;, \quad |\alpha| \not\ni x_1 \;, \quad \alpha \geq 0$

$\Rightarrow \quad r x_1 \sim \alpha$

$\Rightarrow \quad r(x_1 \times C_2) \sim \alpha \times C_2$

$\Rightarrow \quad r(F_1 \cdot F_1) = (F_1 \cdot (\alpha \times C_2)) = 0$

$[F_1 \cap (\alpha \times C_2) = \emptyset]$

similar with F_2

(iii) <u>Fact</u>: C sm proper curve $(k = \bar{k}\,,\; g = g(C))$

D div on C

$\deg(D) \geq 2g+1 \implies D$ is very ample

(see Ha, IV, Cor 3.2)

In part nx_i is very ample on C_i for $n \gg 0$

$$\Rightarrow \quad i_1 : C_1 \hookrightarrow \mathbb{P}_k^{r_1} = P_1$$

$$i_1^* \mathcal{O}_{P_1}(1) \cong \mathcal{O}_{C_1}(nx_1)$$

and. $$i_2 : C_2 \hookrightarrow \mathbb{P}^{r_2} = P_2$$

$$i_2^* \mathcal{O}_{P_2}(1) = \mathcal{O}_{C_1}(nx_2)$$

$\rightarrow$ get closed embd.

$$i : \underset{\overset{\|}{X}}{C_1 \times C_2} \xrightarrow{i_1 \times i_2} P_1 \times P_2 \underset{\substack{\uparrow \\ \text{Segre Embedding}}}{\overset{s}{\hookrightarrow}} \mathbb{P}_k^{r_1 r_2 + r_1 + r_2} = P$$

and $$s^* \mathcal{O}_P(1) = pr_1^* \mathcal{O}_{P_1}(1) \otimes pr_2^* \mathcal{O}_{P_2}(1)$$

$$\Rightarrow i^* \mathcal{O}_P(1) = \mathcal{O}_X(n(F_1 + F_2))$$

$\Rightarrow$ $n(F_1 + F_2)$ sehr ample $\Rightarrow$ $F_1 + F_2$ ample.

$\square$

(2) Thm (Castelnuovo – Severi Inequality)

$X = C_1 \times C_2$ as above

$D \in CH^1(X)$ set $(D.F_i) := d_i$

Then

$$(D.D) \leq 2 d_1 d_2$$

Proof: $A := F_1 + F_2$ ample (1), iii)

$$(A.A) \underset{(1),\, i)}{=} 2 > 0$$

$$\Big(\underbrace{\big(D - d_2 F_1 - d_1 F_2\big)}_{=: D'} . A\Big) = 0$$

$\Longrightarrow$ Hodge Index §10, (17)

$$(D'.D') \leq 0 \qquad \left(\begin{array}{l} \text{"="}\ 0 \text{ if } D' \equiv 0 \\ \text{"<"}\ 0 \text{ else} \end{array}\right)$$

$$\|$$

$$(D.D) - d_2 d_1 - d_1 d_2 - d_2 d_1 + 0 + d_1 d_2 - d_1 d_2 + d_1 d_2 + 0$$

□

③ Def: $X = C_1 \times C_2$, $D \in CH^1(X)$
$d_i := D.F_i$

$$\mathrm{def}(D) := 2d_1d_2 - (D.D) \geq 0$$

defect of D

④ Cor: $D, D' \in CH^1(X)$ $d_i' = D'.F_i$

$$\Rightarrow \quad |(D.D') - d_1d_2' - d_2d_1'| \leq \sqrt{\mathrm{def}(D)\mathrm{def}(D')}$$

Pf: take $m, n \in \mathbb{Z}$

$$0 \leq \mathrm{def}(mD + nD')$$

$$= 2(md_1 + nd_1')(md_2 + nd_2')$$

$$- m^2(D.D) - 2mn(D.D') - n^2(D'.D')$$

$$= m^2\mathrm{def}(D) + n^2\mathrm{def}(D') + 2mn(d_1d_2' + d_1'd_2 - (D.D'))$$

$$2mn((D.D') - d_1d_2' - d_1'd_2) \leq m^2\mathrm{def}(D) + n^2\mathrm{def}(D')$$

$\Rightarrow$ ☐

(5) Prop.: $f : C_1 \to C_2$ dominant morphism.

of degree $n = [k(C_1) : k(C_2)]$

$\Gamma_f = \operatorname{im}(\mathrm{id} \times f : C_1 \to C_1 \times C_2) = $ graph of f

$\subset X$

$$\Rightarrow \quad \deg(\Gamma_f) = 2 g_2 n \quad , \quad g_2 = g(C_2)$$

Pf.: Note Γ_f and F_i intersect properly (for F_1 since f is dom.)

1. $\Gamma_f \cdot F_1 = \sum\limits_{x \in \Gamma_f \cap F_1 = f^{-1}(x_2)} i_x(\Gamma_f, F_1)$

$(F_1 = C_1 \times \{x_2\})$

$x \in f^{-1}(x_2)$, $\gamma, \varphi_1 \in \mathcal{O}_{X,x}$ local eq for Γ_f and F_1

$$\Rightarrow \quad i_x(\Gamma_f, F_1) = \ell\left(\frac{\mathcal{O}_{X,x}}{\gamma, \varphi_1}\right)$$

But

$$\frac{\mathcal{O}_{X_1,x}}{\varphi_1} = \mathcal{O}_{F_1,x} = \mathcal{O}_{C_1,y} \quad \text{with } y = pr_1(x)$$

$pr_1 : C_1 \times C_2 \to C_2$

and $\varphi_1 = pr_2^* \tau$, $\tau \in \mathcal{O}_{C_2,x_2}$ loc param.

$$\mu = pr_1^* f^* \tau - pr_2^* \tau$$

$$\Rightarrow \frac{\mathcal{O}_{X_1,x}}{\varphi_1,\mu} \cong \frac{\mathcal{O}_{C_1,y}}{(f^*\tau)} \Rightarrow i_x(\Gamma_f, F_1) = \ell\left(\frac{\mathcal{O}_{C_1,y}}{f^*\tau}\right)$$

$= e(y/x_2)$

$=$ ramification index

$$\Rightarrow \underbrace{(\Gamma_f \cdot F_1)} = \sum_{y \in f^{-1}(x_2)} e(y/x_2) \cdot \underbrace{f(y/x_2)}_{=1} \overset{\S 6, (7), ii)}{=} \underbrace{n} \quad (*)$$

similar

$$\underbrace{(\Gamma_f \cdot F_2)} = \sum_{x \in \underbrace{\Gamma_f \cap F_2}_{x_1 \times f(x_1)}} i_x(\Gamma_f, F_2) = \underbrace{1} \qquad (2*)$$

$\underset{\text{defn}}{\Rightarrow}$ $\quad \operatorname{def}(T_f) = 2n - (T_f \cdot T_f) \qquad (3*)$

<u>Claim</u> $\quad K_X = (K_{C_1} \times C_2) + (C_1 \times K_{C_2})$

<u>indeed</u>: $\quad pr_2 : X \to C_2$ sm

$$\begin{tikzcd}
0 \arrow[r] & pr_2^* \Omega^1_{C_2/k} \arrow[r] & \Omega^1_{X/k} \arrow[r] & \Omega^1_{X/C_2} \arrow[r] \arrow[d, equal] & 0 \\
& & & pr_1^* \Omega^1_{C_1/k} &
\end{tikzcd}$$

exact (see CSS, §11, (10))

(CSS, §11, (15))

$$\underset{\text{CSS, §13, (4)}}{\Rightarrow} \quad \underset{\substack{\| \\ \mathcal{O}(K_X)}}{\omega_{X/k}} \cong \underset{\substack{\| \\ \mathcal{O}_X(K_{C_1} \times C_2)}}{pr_1^* \omega_{C_1}} \otimes \underset{\substack{\| \\ \mathcal{O}_X(C_1 \times K_{C_2})}}{pr_2^* \omega_2} \quad \Rightarrow \text{Claim.}$$

$T_f \subset X$ sm curve, $\cong C_1 \to g(T_f) = g_1 := g(C_1)$

$$\underset{\substack{\text{§10, (4)} \\ \text{(adjunction formula)}}}{\Rightarrow} \quad 2g_1 - 2 = ((K_X + T_f) \cdot T_f)$$

$$= (T_f \cdot T_f) + (K_{C_1} \times C_2) \cdot T_f + (C_1 \times K_{C_2}) \cdot T_f \qquad (4*)$$

and

$$K_{C_2} = \sum r_i\, g_i$$

$$\Rightarrow\quad C_1 \times K_{C_2} = \sum r_i\, \overset{C_1\times\{g_i\}}{\overset{\shortparallel}{F_{1,g_i}}}$$

$$\underset{(*)}{\Rightarrow}\quad (K_{C_2}\cdot \Gamma_f) = \sum r_i\, n = n \deg K_{C_2}$$
$$= n(2g_2-2)$$

similar (with (2*))

$$(K_{C_1}\cdot \Gamma_f) = (2g_1-2)$$

$$\underset{(4*)}{\Rightarrow}$$

$$(\Gamma_f\cdot\Gamma_f) = -(2g_2-2)\, n$$

$$\underset{(3*)}{\Rightarrow}\quad \deg(\Gamma_f) = 2n + (2g_2-2)n = 2ng_2$$

$\square$

Now assume

$\mathbb{F}_q$ = finite field with q - Elts

$k = \overline{\mathbb{F}_q}$ = alg closure

C sm proj, geom connected curve$/k_0$

$\varphi : C \to C$ q - power Frobenius

i.e. $\varphi^* : \mathcal{O}_C \to \mathcal{O}_C$, $a \mapsto a^q$

Note $\varphi^*_{|\mathbb{F}_q} = \mathrm{id}$

$\Rightarrow$
$$\begin{tikzcd} C \arrow[rr, "\varphi"] \arrow[dr] & & C \arrow[dl] \\ & \operatorname{Spec} \mathbb{F}_q & \end{tikzcd}$$
commutes

$\Rightarrow$ $\overline{\varphi} : \overline{C} := C \underset{\mathbb{F}_q}{\otimes} k \xrightarrow{\varphi \times \mathrm{id}} \overline{C}$

6. Key-lemma: $n \geq 1$
$$\Gamma = \text{graph of } \bar{\varphi}^n \subset \bar{C} \times \bar{C} =: X$$
$$\Delta = \text{diagonal} \subset \bar{C} \times \bar{C}$$

$$\Rightarrow (\Gamma \cdot \Delta) = |C(\mathbb{F}_{q^n})|$$

Pf: $U = \operatorname{Spec} A \subset C$ open with
$$A = \frac{\mathbb{F}_q[X_1, \dots, X_r]}{I}$$

$$\Longrightarrow \quad \Gamma \cap \Delta \cap U = \operatorname{Spec} B$$

with
$$B = \frac{k[x_1, \dots, x_r, y_1, \dots, y_r]}{(I(x), I(y), x_i - y_i, x_i - y_i^{q^n}, i = 1 \dots r)}$$
$$\cong \frac{k[x_1 \dots x_r]}{(I, x_i^{q^n} - x_i, i = 1, \dots r)}$$

Note
$$x_i^{q^n} - x_i = \prod_{\lambda \in \mathbb{F}_{q^n} \subset k} (x_i - \lambda)$$

$$\Rightarrow \operatorname{Spec} B = \bar{U}(k) \cap \mathbb{A}^r_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^n}) = U(\mathbb{F}_{q^n}) \quad \text{finite}$$

$\Rightarrow$ Γ and Δ meet properly, $\Gamma \cap \Delta = C(\mathbb{F}_{q^n})$
$\mathcal{U}$ arbitr. (scheme theoretic)

and $i_x(\Gamma, \Delta) = \ell(B_x) = \ell(B/m_x) = 1$
$x \in \Gamma \cap \Delta \cap \mathcal{U}$

$x = (X_1 - \lambda_1, \dots, X_r - \lambda_r)$

$$\Rightarrow (\Gamma \cdot \Delta) = \sum_{x \in \Gamma \cap \Delta} i_x(\Gamma, \Delta) = |C(\mathbb{F}_{q^n})|$$

$\square$

(7) Lemma: $\bar{\varphi}^n : \bar{C} \longrightarrow \bar{C}$ as above, $K = \mathcal{R}(\bar{C})$
($\mathcal{R}$-linear q^n-power-Frobenius)

$$\Rightarrow \deg \bar{\varphi}^n = [K : \mathcal{R}(K^{q^n})] = q^n$$

Pf: $\bar{C}$ sm$/\mathcal{R}$ $\underset{\text{CSS §11, (18)}}{\Rightarrow}$ $\exists\, t \in K$ transc s.t.
$K \supset \underbrace{\mathcal{R}(t)}_{=K_0}$ finite sep.

$\underset{\text{Algebra}}{\Rightarrow}$ $K = K_0[K^p] = \dots = K_0[K^{q^n}] = \mathcal{R}(t)[K^{q^n}]$

$\mathcal{R}(K^{q^n}) = \mathcal{R}(K_0^{q^n}([K^{q^n}])) = \mathcal{R}(t^{q^n})[K^{q^n}]$

$$\Rightarrow K \cong \frac{\mathcal{R}(K^{q^n})[T]}{T^{q^n} - t^{q^n}} \Rightarrow \deg \bar{\varphi}^n = q^n$$

$\square$

Recall (§8, 7)

<u>Main Thm</u>: $C/\mathbb{F}_q$ as above, $g = g(C)$

$$\Longrightarrow \quad \left| 1 + q^n - |C(\mathbb{F}_{q^n})| \right| \leq 2g\sqrt{q^n}$$

<u>Pf</u>: $\bar{C} = C \otimes_{\mathbb{F}_q} k$, Γ', Δ as in 6, 7

$$5 \Rightarrow \operatorname{def}(\Delta) = 2g$$

$$5, 7 \Rightarrow \operatorname{def}(\Gamma') = 2g\, q^n$$

$x \in \bar{C}$ some pt.

$F_1 = \bar{C} \times \{x\}$, $F_2 = \{x\} \times \bar{C}$,

$(\Delta \cdot F_i) = 1$, $i = 1, 2$, $(\Gamma' \cdot F_1) = q^n$ (by 7 and $(*)$ in pf of 5)

$(\Gamma' \cdot F_2) = 1$ (by $2(*)$ in pf of 5)

$$4 \Longrightarrow \left| \underbrace{(\Gamma' \cdot \Delta)}_{\overset{6}{=}\, |C(\mathbb{F}_{q^n})|} - q^n - 1 \right| \leq \sqrt{\operatorname{def}(\Gamma') \operatorname{def}(\Delta)} = 2g\sqrt{q^n}$$

$\square$