A GEOMETRIC VIEW ON CONGRUENCES OF MODULAR FORMS

§1. Introduction

(PERHAPS) APOCRYPHAL QUOTE ASCRIBED TO M. EICHLER:

'THERE ARE FIVE FUNDAMENTAL OPERATIONS IN MATHEMATICS: ADDITION, SUBTRACTION, MULTIPLICATION, DIVISION AND MODULAR FORMS'

$\boxed{\sim 1750}$ FAGNANO, EULER ETC

FIRST EMBRIONAL APPEARENCE OF MODULAR FORMS

STUDY OF ELLIPTIC INTEGRALS

$$k = 1 - \frac{n^2}{m^2}$$

$$\int_a^b \frac{1}{\sqrt{(1-x^2)(1-k^2x^2)}} \qquad \frac{x^2}{m^2} + \frac{y^2}{n^2} = 1$$

$\boxed{\sim 1820.}$ ABEL AND JACOBI STARTED STUDYING INVERSION OF ELLIPTIC INTEGRALS

$\rightarrow$ LED TO STUDY OF FIRST ELLIPTIC FUNCTIONS

$$u = \int_{x_0}^{x} \frac{d}{\sqrt{4t^3 - g_2 t - g_3}}, \qquad x(u) = \wp(u)$$

WEIERSTRASS $\wp$-FUNCTION

SATISFYING A DIFFERENTIAL EQUATION $(\wp'(u))^2 = 4\wp(u)^3 - g_2\wp(u) - g_3$

MEROMORPHIC FUNCTIONS THAT ARE 'DOUBLY PERIODIC'

MODULAR FORMS (FIRST ATTEMPT)

COMPLEX ANALYTIC FUNCTIONS W/ LARGE NUMBER OF SYMMETRIES

FUNCTIONS SO SYMMETRIC AND REGULAR THAT THEY SHOULD NOT EXISTS!

CONSIDER THE FOLLOWING HOLOMORPHIC FUNCTION ON THE UPPER HALF COMPLEX PLANE $\mathcal{H}$

$$G_{2k}(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0,0\}} (m+nz)^{-2k}, \qquad k \geq 2 \quad \text{ABSOLUTELY CONVERGENT}$$

SATISFIES FOLLOWING SYMMETRIC PROPERTY

$$\forall \gamma \in SL_2\mathbb{Z}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad a,b,c,d \in \mathbb{Z}$$

$$G_{2k}\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} G_{2k}(z)$$

IN PARTICULAR, $G_{2k}(z+1) = G_{2k}(z) \Rightarrow$ CONSIDER ITS FOURIER EXPANSION

$$G_{2k}(q) = 2\zeta(2k)\left(1 - \frac{4k}{B_{2k}} \sum_{n\geq 1} \sigma_{2k-1}(n) q^n\right) \qquad q = \exp(2\pi i z)$$

ANALYTIC/PERIOD ARITHMETIC

$$\sigma_{2k-1}(n) = \sum_{\substack{d|n \\ d>0}} d^{2k-1}$$

B_{2k} BERNOULLI NUMBERS

FACT

$$\wp(z) = \frac{1}{z^2} + \sum_{k\geq 1} (2k+1) G_{2k+2}(z) \cdot z^{2k}$$

$E_{2k}(z) := \frac{1}{2\zeta(2k)} G_{2k}(z)$ NORMALIZED EISENSTEIN SERIES

REM THE COEFFICIENTS ARE RATIONAL NUMBERS!

⇝ MODULAR FORMS HAVE AN ALGEBRAIC NATURE

▶▶ FAST FORWARD

$\sim$ 1960's – NOW   CONNECTION W/ DIOPHANTINE PROBLEMS

- FERMAT'S LAST THEOREM – TAYLOR, WILES ET AL. $X^n + Y^n = Z^n$
- MAZUR'S THEOREM – TORSION SUBGROUPS OF ELLIPTIC CURVES $/\mathbb{Q}$
- GROSS-ZAGIER, KOLYVAGIN'S THEOREM – BSD CONJECTURE

CENTRAL OBJECT IN MODERN NUMBER THEORY

§2. THREE PERSPECTIVES ON MODULAR FORMS

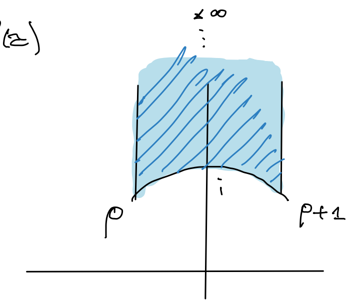
(i) COMPLEX ANALYTIC

$f : \mathcal{H} \longrightarrow \mathbb{C}$ HOLOMORPHIC FUNCTION,

$\forall \gamma \in \Gamma \leqslant SL_2\mathbb{Z}$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$

+ GROWTH CONDITIONS AT INFINITY

⇝ f IS MODULAR FORM OF WEIGHT k WRT Γ



(ii) COMBINATORIAL

$f(q) = \sum_{n \geq 0} a_n q^n$ FOURIER EXPANSION

⇝ GENERATING SERIES

EG
- EISENSTEIN'S SERIES $G_{2k}(q)$ (NUMBER THEORETIC FLAVOUR)
- DEDEKIND'S ETA FUNCTION (COMBINATORIAL FLAVOUR)

$$\eta(q)^{-1} = q^{1/24} \prod_{n \geq 1} (1-q^n)^{-1} = q^{1/24} \sum_{n \geq 0} p(n) q^n,$$

$$p(n) = \#\{\text{PARTITIONS OF } n\}$$

- Modularity theorem (geometric flavour)

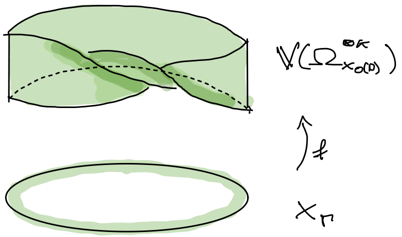
$$f(q) = q\cdot \prod (1-q^n)^2 \prod (1-q^{11\cdot n})^2 = \eta(q)^2\cdot\eta(11q)^2 = \sum_{n\geq 1} a_n q^n$$

$a_p = p+1 - \#(E_f(\mathbb{F}_p))$ for elliptic curve

$E_f : \; y^2+y = x^3-x^2$

(iii) Geometric

$f \in \Gamma(X_\Gamma, \Omega_{X_\Gamma}^{\otimes k})$



X_Γ modular curve

over $\mathbb{C}$ $\rightsquigarrow$ $X_\Gamma = \Gamma\backslash\mathcal{H}^*$.

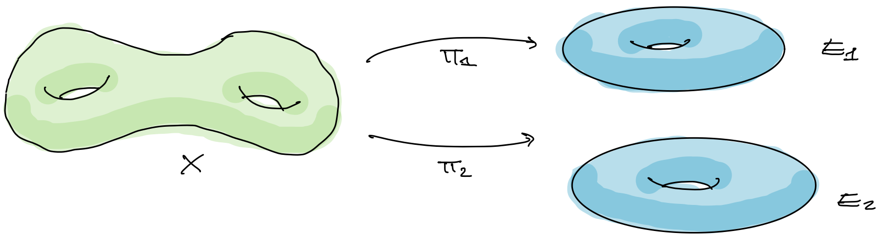
§3. (Intermezzo) Two elliptic curves of conductor 37

Consider

$E_1 : \; y^2 = x^3 - 16x + 16$ $\qquad$ $E_2 : \; y^2 = x^3 - 2427840x - 1456056432$

$X : \; y^2 = x^6 + 8x^5 - 20x^4 + 28x^3 - 24x^2 + 12x - 4$ $\quad$ genus 2-curve

$X(\mathbb{C}) \simeq \Gamma_0(37)\backslash\mathcal{H}^*$ $\qquad$ $\Gamma_0(37) = \{\gamma \in SL_2\mathbb{Z} \mid \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod 37\}$



Jacobian of X, $\quad J(X) \sim E_1 \times E_2$

$\Gamma(X, \Omega^1_X) \otimes \mathbb{C} = \mathbb{C}f_1 \oplus \mathbb{C}f_2$ $\quad$ f_1, f_2 modular forms w/ integer coeff.

$$\boxed{a_p(f_i) = p+1 - \#(E_i(\mathbb{F}_p)) \qquad p \neq 37}$$

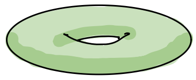
Instance of Tanyama-Shimura modularity,
fundamental piece of proof of Wiles approach to Fermat last theorem

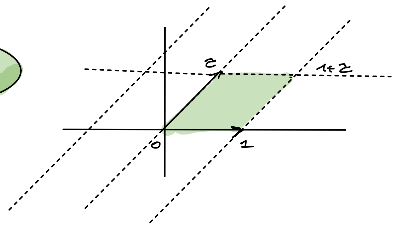
[!] Fourier expansions of modular forms encode deep arithmetic information

§ 4. NEW FUNKY CONGRUENCE RELATION

TO EVERY ELLIPTIC CURVE $C/\mathbb{Q}$ WE CAN ASSOCIATE j-INVARIANT

$$C(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + z\mathbb{Z}) \quad \text{COMPLEX TORUS}$$





$$\boxed{j(z) := 1728 \frac{E_4(z)^3}{E_4(z)^3 - E_6(z)^2}}$$

IT HAS A FAMOUS q-EXPANSION

$$j(q) = \frac{1}{q} + 744 + 196884\, q + 21493760\, q^2 + \dots$$

TURNS OUT, VALUE j IDENTIFIES UNIQUELY ELLIPTIC CURVES UP TO ISOMORPHISM $/\mathbb{C}$

PENGCHENG ZHANG (2025) OBSERVED NUMERICALLY CURIOUS BEHAVIOUR OF MEROMORPHIC MODULAR FORMS

$$a_p\left(E_k(q) \big/ j(q) - j(C)\right) \equiv a_p(C) \mod p \qquad \forall\, k \in \{4,6,8,10,14\}$$

EVEN STRONGER CONGRUENCES HOLD WHEN WE CONSIDER THE VECTOR SPACE SPANNED BY

$$E_k(q) \big/ (j(q) - j(C))^i \qquad i = 1, \dots, k-1$$

<u>EG</u> $C/\mathbb{Q}$: $y^2 + xy = x^3 - x^2 - 2x - 1$, $j(C) = -3375$

CONSIDER THE FOLLOWING MEROMORPHIC MODULAR FORMS

- $f_1 = \dfrac{E_4}{j + 3375}$
- $f_2 = 19 \cdot \dfrac{E_4}{j+3375} - 91125 \dfrac{E_4}{(j+3375)^2}$
- $f_3 = 1399 \cdot \dfrac{E_4}{j+3375} - 19008675 \dfrac{E_4}{(j+3375)^2} + 54251268750 \cdot \dfrac{E_4}{(j+3375)^3}$

THEN WE OBSERVED THAT FOR EVERY (ORDINARY) $p > 3$, FOR EVERY $\ell > 0$

$$\boxed{\begin{cases} a_{np^{\ell+1}}(f_1) \equiv \alpha_p(C)^2\, a_{np^\ell}(f_1) \mod p^{3\ell} \\ a_{np^{\ell+1}}(f_1) \equiv \alpha_p(C)\,\beta_p(C)\, a_{np^\ell}(f_1) \mod p^{3\ell} \\ a_{np^{\ell+1}}(f_1) \equiv \beta_p(C)^2\, a_{np^\ell}(f_1) \mod p^{3\ell} \end{cases}}$$

WHERE $\alpha_p(C), \beta_p(C)$ ARE p-ADIC ROOTS OF $X^2 - a_p(C)X + p$

! WHY ON EARTH $E_k/(j - j(C))$ SHOULD KNOW ABOUT REDUCTION MODULO p OF C ?

⇝ DEEP AND HIDDEN INTERACTION IN ARITHMETIC GEOMETRY OF MODULAR CURVE

§ 5. Geometry of modular curves

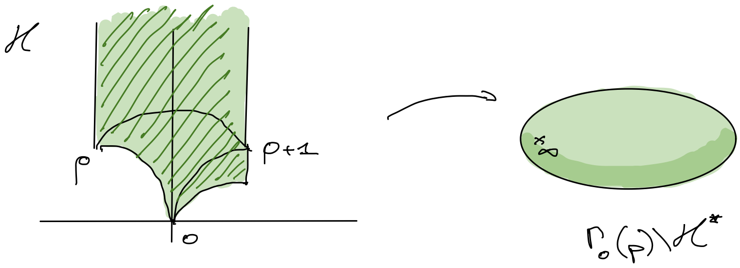
- Complex picture

$\Gamma_0(p) = \{ \gamma \in SL_2\mathbb{Z} : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \}$ congruence subgroup

$Y_0(p) := \Gamma_0(p) \backslash \mathcal{H} \longrightarrow \{ \text{elliptic curves}/\mathbb{C} \text{ w/ } p\text{-torsion subgp.} \}/_\cong$

$[\tau] \longmapsto (\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}), \langle \tfrac{1}{p} \rangle)$

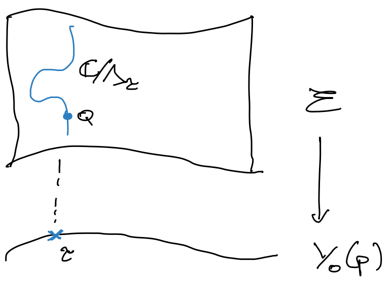
$X_0(p)$ compactification $\rightsquigarrow$ Riemann surface



$\Gamma_0(p) \backslash \mathcal{H}^*$

Incorporate in the picture the elliptic curves parametrized

$\rightsquigarrow$ universal elliptic curve $\mathcal{E} = \Gamma_0(p) \backslash \mathcal{H} \times \mathbb{C} / \mathbb{Z}^2$



- Algebro-geometric picture

$[\Gamma_0(p)] : \underline{\text{Rings}} \longrightarrow \underline{\text{Sets}}$

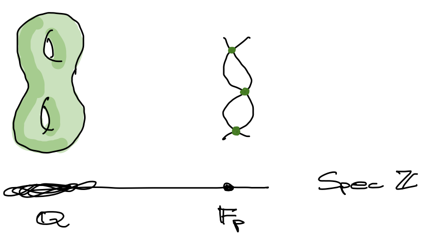
Need extra data for fine representability

$R \longmapsto \{ E/R \text{ elliptic curve w/ } p\text{-torsion subgroup} \}$

Functor (almost) represented by smooth affine scheme $Y_0(p)$ over $\mathbb{Z}[1/p]$

↳ arithmetic info

Deligne - Rapaport model: minimal model over $\mathbb{Z}$

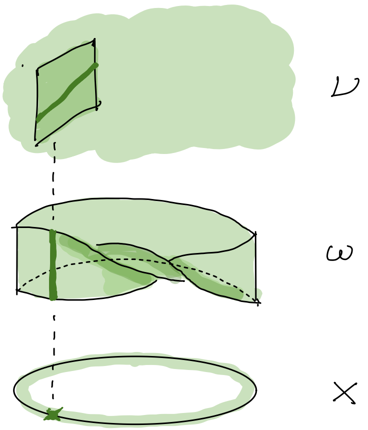


§6. Cohomological description

Consider $\mathcal{E} \xrightarrow[\pi]{} X$ universal elliptic curve

$$\omega := \pi_* \Omega^1_{\mathcal{E}/Y}$$ Hodge line bundle ⇝ extends to X

$$\mathcal{V} := R^1 \pi_* \Omega^\bullet_{\mathcal{E}/Y}$$ Relative de Rham cohomology
rank 2 vector bundle



Fiberwise, for every α rational point in X

$$\alpha^* \omega = \Gamma^0(\mathcal{E}_\alpha, \Omega^1_{\mathcal{E}_\alpha})$$ global differential

$$\alpha^* \mathcal{V} = H^1_{dR}(\mathcal{E}_\alpha)$$ de Rham cohomology of $\mathcal{E}_\alpha$

sitting in exact sequence

$$0 \to H^0(\mathcal{E}_\alpha, \Omega^1_{\mathcal{E}_\alpha}) \longrightarrow H^1_{dR}(\mathcal{E}_\alpha) \longrightarrow H^1(\mathcal{E}_\alpha, \mathcal{O}_{\mathcal{E}_\alpha}) \to 0$$

This extends to vector bundle over X

$$0 \longrightarrow \omega \longrightarrow \mathcal{V} \longrightarrow \omega^{-1} \longrightarrow 0$$

and to symmetric powers $\mathcal{V}_k = \mathrm{Sym}^k \mathcal{V}$ giving filtration

$$\mathcal{V}_k = F^0\mathcal{V}_k \supseteq F^1\mathcal{V}_k \supseteq \dots \supseteq \underset{\substack{\cong \\ \omega^{\otimes k}}}{F^k\mathcal{V}_k} \supseteq F^{k+1}\mathcal{V}_k = 0$$

It can be shown

$$f \in \Gamma^0(X, \omega^{\otimes k})$$ is a modular form of weight k

The relative de Rham cohomology $\mathcal{V}$ comes equipped with a connection

$$\nabla : \mathcal{V}_k \longrightarrow \mathcal{V}_k \otimes \Omega^1_X(\log C)$$ called Gauss–Manin connection

C set of cusps

We can then study modular forms from an $\boxed{\text{Hodge – theoretic point of view}}$

(unfortunately: relative context, cohomology w/ coefficients, logarithmic singularities)

Recall Pengcheng's congruences:
relate

coefficients meromorphic modular forms w/ prescribed poles

$\updownarrow$

characteristic polynomial of Frobenius on cohomology of elliptic curves

We can use the Gysin sequence

Let $\alpha \in X(\mathbb{Q})$ rational point corresponding to elliptic curve $\mathcal{E}_\alpha$

$$U = X \setminus \{\alpha\}$$

For $k \geq 2$ we have an exact sequence

$$\boxed{0 \longrightarrow H^1_{dR}(X, \mathcal{V}_k) \longrightarrow H^1_{dR}(U, \mathcal{V}_k) \xrightarrow{\text{Res}} H^0(\alpha^* X, \mathcal{V}_k) \longrightarrow 0 \qquad H^0(\alpha^* X, \mathcal{V}_k) \cong \mathrm{Sym}^k H^1_{dR}(\mathcal{E}_\alpha)(1)}$$

Lemma For $k \geq 2$ we have the following isomorphism

$$H^1_{dR}(U, \mathcal{V}_k) \simeq \Gamma(U, \omega^{\otimes k+2}) / \mathcal{D}^{k+1}\left(\Gamma(U, \omega^{\otimes -k})\right)$$

where $\mathcal{D}$ is the Bol operator

$$\mathcal{D} f(q) = q \frac{d}{dq} f(q) = \sum_{n \geq 0} n a_n q^n, \qquad f(q) = \sum_{n \geq 0} a_n q^n$$

In particular, every class in $H^1_{dR}(U, \mathcal{V}_k)$ can be represented by the class of a meromorphic modular form of weight $k+2$

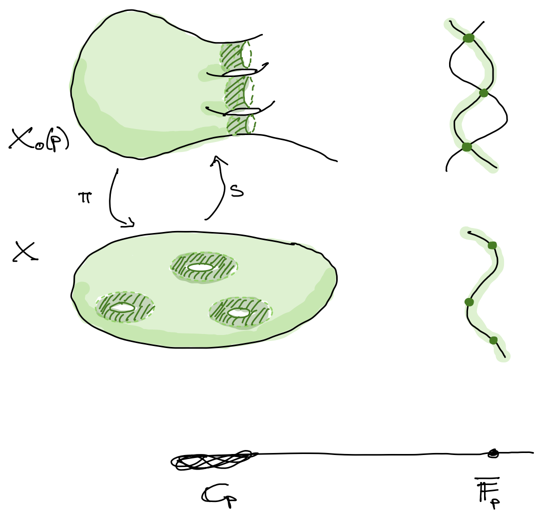
Last missing piece: Frobenius action

§7. p-adic perspective

To understand the relation between the

- global char 0 $\rightsquigarrow$ meromorphic MF
- reduction char p $\rightsquigarrow$ Frobenius

We need to change topology $\rightsquigarrow$ rigid geometry



In this realm, Frobenius has natural moduli description

By Katz's fundational result on p-adic MF section s given by canonical subgroup

$$X \longrightarrow X_0(p)$$

$$E \longmapsto (E, K_E)$$

w/ K_E specific p-subgroup

reduction coincides w/ kernel of reduction modulo p of p-torsion points.

ON MODULAR FORMS WE HAVE TWO OPERATORS INVOLVING p

- $V_p : f(q) \longmapsto f(q^p) = \sum_{n \geq 0} a_n q^{np}$
- $U_p : f(q) \longmapsto \sum_{n \geq 0} a_{np} q^n$

THESE OPERATORS CAN BE REALIZED AS PULL BACK ALONG SECTION s AND ITS TRACE

⇝ PROMOTE THIS ACTION TO COHOMOLOGY

$$H^1_{dR}(U, \mathcal{V}_k) \quad \circlearrowright \; [V_p] = \mathrm{Frob} \qquad \circlearrowleft \; [U_p] = \mathrm{Vers}$$

SUCH THAT $\mathrm{Frob} \circ \mathrm{Vers} = p^{k+1}$

THE GYSIN SEQUENCE HAS AN HIDDEN FROBENIUS STRUCTURE COMING FROM THE MODEL OF THE MODULAR CURVE AND ITS RIGID GEOMETRY

$$0 \longrightarrow \underset{\circlearrowright \,\mathrm{Frob}}{H^1_{dR}(X, \mathcal{V}_k^{rig})} \longrightarrow \underset{\circlearrowright \,\mathrm{Frob}}{H^1_{dR}(U, \mathcal{V}_k^{rig})} \xrightarrow{\mathrm{Res}} \underset{\circlearrowright \,\mathrm{Frob}}{\mathrm{Sym}^k H^1_{dR}(\mathcal{E}_\alpha)(1)} \longrightarrow 0$$