Arithmetic algebraization à la ①

Z.GAD – Chudnovsky II. Diophantine applications

① Isogeny between elliptic curves

$E/\mathbb{Q}$ ell. curve with good reduction over $\mathrm{Spec}\,\mathbb{Z}[\frac{1}{N}]$.

$\mathcal{E} \to \mathrm{Spec}\,\mathbb{Z}[\frac{1}{N}]$ its regular model

Fact: the p^{th} power map on Lie $\mathcal{E}/\mathbb{F}_p$ is multiplication

by $a_p(E) = p+1-|\mathcal{E}(\mathbb{F}_p)|$. (Hasse-Weil)

Theorem. For any $E, E'/\mathbb{Q}$, the foll. are equivalent

1) E and E' are isogenous over $\mathbb{Q}$

2) $a_p(E) = a_p(E')$ for almost all p.

Proof. $G = E \times E'$. To give an isogeny over $\mathbb{Q}$

is equivalent to give a subgroup H of G of

dim 1 surjecting to both factors.

$\mathfrak{h} \subseteq \mathrm{Lie}(G) = \mathrm{Lie}\,E \oplus \mathrm{Lie}\,E'$

of dim 1, distinct from $\mathrm{Lie}\,E \oplus \{0\}$, $\{0\} \oplus \mathrm{Lie}\,E'$

Let $N \in \mathbb{N}$ such that $\mathcal{E}, \mathcal{E}' \to \mathrm{Spec}\,\mathbb{Z}[\frac{1}{N}]$ models

Then $a_p(E) = a_p(E') \overset{|a_p(E)| \le 2\sqrt{p}}{\Longleftrightarrow} a_p(E) \equiv a_p(E') \mod p$

for $p \gg 0$

$\Longleftrightarrow$ $\mathfrak{h}$ is stable under p^{th} power
Fact

$\Longleftrightarrow$ $\mathfrak{h}$ is algebraic, i.e. $\mathfrak{h} = \mathrm{Lie}\, H$
Theorem B
for $H < G$

$\Longleftrightarrow$ $E \underset{\text{isog}}{\sim} E'$ over $\mathbb{Q}$ $\square$

② Grothendieck-Katz conjecture

Background:

Consider the following linear differential system $\frac{d}{dz} Y = A(z) Y$

$A(z) \in M_d(\mathbb{Q}(z))$

Goal: give a criterion for a system to have a basis of algebraic solutions, i.e. the holomorphic solutions on a neighborhood of $z_0 \in \mathbb{Q}$. (z_0 not a pole of $A(z)$) are algebraic over $\mathbb{Q}(z)$.

Conjecturally, this criterion is:

(*) For almost all p, $\frac{d}{dz} Y = A(z) Y$ mod p

has a basis of alg. solutions over $\mathbb{F}_p(z)$.

(*) can be verified

<u>Lemma</u>: Define $\begin{cases} A_0(z) = Id \\ A_1(z) = A(z) \\ A_{n+1}(z) = \frac{d}{dz} A_n(z) + A_n(z) A(z) \end{cases}$

Then TFAE:

1) $\frac{d}{dz} Y = A(z) Y$ mod p has a basis of algebraic solutions over $\mathbb{F}_p(z)$

2) ——— solutions in $\mathbb{F}_p(z)$

3) ——— solutions in $\mathbb{F}_p((z))$

4) $A_p \equiv 0$ mod "p-curvature"

<u>Proof</u> 1) $\Rightarrow$ 2) $\Rightarrow$ 3) ✓

3) $\Rightarrow$ 4) $Y(z)$ is a solution $\Rightarrow \frac{d^n}{dz^n} Y(z) = A_n(z) Y(z)$

$Y(z)$ is a solution in $\mathbb{F}_p((z))$ $\rightarrow \frac{d^p}{dz^p} Y(z) = 0$ mod p.

$\Rightarrow A_p \equiv 0 \mod p$

4) $\Rightarrow$ 1) $\quad Y(z) = \left(\sum_{i=0}^{p-1} \frac{(-z)^i}{i!} A_i(z) \right)^{-1}$

is a basis of solutions in $\mathbb{F}_p(z)$.

2) <u>Statement</u>

<u>Conjecture</u>: X smooth quasi-projective $/K$ number field

(E, ∇) vector bundle $/X$ with integrable connection

If for almost all p, the p-curvature of (E, ∇) mod p vanishes, then $\exists$ finite étale map $f : Y \to X$ such that $f^* E =$ trivial.

Ex<u>planation</u>:

E vector bundle $/X$ $\quad X$ over k

$\mathcal{E}$ = sheaf of sections

<u>connection</u>: K-linear map $\nabla : \mathcal{E} \to \mathcal{E} \otimes_{\mathcal{O}_X} \Omega^1_X$

such that: $\forall\, \mathcal{U} \hookrightarrow X$, $\forall e \in \Gamma(\mathcal{U}, \mathcal{E})$, $f \in \Gamma(\mathcal{U}, \mathcal{O}_X)$

$$\nabla(fe) = f \nabla e + e \otimes df$$ leibniz rule

3

Remark: (1) $\nabla_1, \nabla_2 \in Hom_k(\mathcal{E}, \Omega^1_X(\mathcal{E}))$ connections

Leibniz $\Rightarrow$ $\nabla_1 - \nabla_2 \in Hom_{\mathcal{O}_X}(\mathcal{E}, \Omega^1_X(\mathcal{E}))$.

Conversely, given a connection ∇_0 and

$\gamma \in Hom_{\mathcal{O}_X}(\mathcal{E}, \Omega^1_X(\mathcal{E}))$

$\nabla_0 + \gamma$ is a connection

$\Rightarrow$ {connections on E} is a principal homogeneous space under $Hom_{\mathcal{O}_X}(\mathcal{E}, \Omega^1_X(\mathcal{E}))$. (can be empty)

(2) We can extend ∇ to

$$\nabla_i : \mathcal{E} \otimes_{\mathcal{O}_X} \Omega^i_X \longrightarrow \mathcal{E} \otimes_{\mathcal{O}_X} \Omega^{i+1}_X \qquad i \geq 0$$

by $\nabla_i(fe) = (-1)^i f \nabla e + e \otimes df \quad f \in \Gamma(U, \Omega^i_X)$

Fact: $\{(E, \nabla)\}$ flat regular singular $\xrightarrow{\text{equiv}}$ representations of $\pi_1(X)$

The curvature of ∇ is $\Psi(E, \nabla) = \nabla_1 \circ \nabla \quad (= \nabla^2)$

Remark: $\nabla^2 : \mathcal{E} \to \mathcal{E} \otimes \Omega^1_X$ always $\mathcal{O}_X$-linear

so $\nabla^2 \in End(\mathcal{E}) \otimes_{\mathcal{O}_X} \Omega^2_X$

∇ integrable if one of the following equivalent conditions hold

1) $TX \to End(\mathcal{E})$ homomorphism of Lie algebras

2) $\Psi(E, \nabla) = 0$.

p-curvature:

$char(k) = p > 0$

(E, ∇) is integrable

Def. The p-curvature $\Psi_p(E, \nabla)$

$$TX \longrightarrow End(\mathcal{E})$$
$$\partial \longmapsto \nabla(\partial)^p - \nabla(\partial^p)$$

Remark: $\Psi_p(E, \nabla)(f_1 \partial_1 + f_2 \partial_2)$

$$= f_1^p \Psi_p(E, \nabla)(\partial_1) + f_2^p \Psi_p(E, \nabla)(\partial_2)$$

Theorem (Cartier) TFAE

1) $\Psi_p = 0$

2) $TX \to End(\mathcal{E})$ $\partial \mapsto \nabla(\partial)$ is a homomorphism of p-Lie algebra

3) (E, ∇) is trivial [or equivalently, $\mathcal{E}$ is generated by $\mathcal{E}^{\nabla} = \{e \in \mathcal{E} \mid \nabla e = 0\}$ as $\mathcal{O}_X$-module)

Andrè's Theorem:

Prop. $(E, \nabla)/_X$ int. connection $X/_K$ number field

$\langle E, \nabla \rangle^{\otimes}$ = category of ∇-stable subquotients of all tensor products $E^{\otimes m} \otimes (E^{\vee})^{\otimes n}$

X connected $\Rightarrow$ $\langle E, \nabla \rangle^{\otimes}$ Tannakian

Def. The generic diff. Galois group G of (E, ∇) is the subgroup of $GL(E \otimes K(X))$ stabilizing all objects of $\langle E, \nabla \rangle$.

$\forall K \hookrightarrow \mathbb{C}$ $(E^{an}, \nabla^{an})/_{X(\mathbb{C})}$

Galois diff. group = Zariski closure of image $(\pi_1(X(\mathbb{C}), x) \to GL(E_x))$ $\forall x \in X(\mathbb{C})$

Theorem (André)

The Grothendieck–Katz conjecture holds if the Galois diff. group G of (E, ∇) is virtually solvable.

Proof

Step 1: reduce to $\dim X = 1$

$\exists\, C \hookrightarrow X$ curve

$$\begin{array}{ccc} \pi_1(C, x) & \longrightarrow & \pi_1(X, x) \\ & & \downarrow \\ & & GL(E_x) \end{array}$$

Problem: invariable property fails for $\mathcal{E}^{\nabla}$

Step 2: replace X by $S^k X$ ← G is solvable

dévissage ⇝ We may assume G is connected commutative

$E^k \longrightarrow X^k$

G^k-bundle

$\mathrm{sm}: G^k \to G$

$(\mathrm{sum})_* \, E^k/S^k \to X^k/S^k$

Step 3: For $k \gg 0$, the Lindelöf property holds because $S^k X$ "looks like" $\mathrm{Jac}_D(\bar{X})$
birational □

③

Theorem: X = geometric connected smooth projective curve $/K$

$P \in X(K)$ $\quad \varphi \in \hat{\mathcal{O}}_{X,P}$ formal function around P such that the formal graph of φ in $\widehat{X \times \mathbb{A}^1}_{(\Gamma, \varphi(P))}$ is A-analytic

$\Omega \subseteq X(\mathbb{C})$ with some property

If $\widehat{\deg}\,(T_P X, \|\cdot\|^{\mathrm{cap}}_{\Omega}) > 0$, then φ is the formal germ of Γ of a rational function on X.