Last time

Existence of an ab. var. $A/\mathbb{Q}$ satisfying certain properties (depending on a prime N) $\Rightarrow$ $\nexists$ ell. curve $/\mathbb{Q}$ w/ pt. of order N

This time

Thm B: $A/\mathbb{Q}$ ab var. N, p distinct prime ; N odd. Suppose
1) A has good redn away from N
2) A has toric redn at N
3) The Jördan – Hölder constituents of $A[p](\bar{\mathbb{Q}})$ as a $G_{\mathbb{Q}}$-mod. are 1-dim. & either trivial or cyclotomic.

§1. Classical Descent

Recall: weak Mordell–Weil Thm: $A(\mathbb{Q})/nA(\mathbb{Q})$ fin.

Pf: Consider

$$0 \to A[n] \to A \xrightarrow{\times n} A \to 0$$

LES

$$0 \to A(\mathbb{Q})[n] \to A(\mathbb{Q}) \xrightarrow{n} A(\mathbb{Q}) \to H^1(\mathbb{Q}, A[n]) \to H^1(\mathbb{Q}, A) \xrightarrow{n} H^1(\mathbb{Q}, A) \to \cdots$$

$\Rightarrow$ SES

$$0 \to A(\mathbb{Q})/nA(\mathbb{Q}) \to H^1(\mathbb{Q}, A[n]) \to H^1(\mathbb{Q}, A)[n] \to 0$$

$\downarrow \qquad \downarrow$ not fin. $\qquad \downarrow$

Impose local conditions

$$0 \to A(\mathbb{Q}_v)/nA(\mathbb{Q}_v) \to H^1(\mathbb{Q}_v, A[n]) \to H^1(\mathbb{Q}_v, A)[n] \to 0$$

See Ch.10 Thm 4.2 of Silverman

Consider subgp of $H^1(\mathbb{Q}, A[n])$ given by elts that map to the image L_v of $A(\mathbb{Q})/nA(\mathbb{Q})$ in $H^1(\mathbb{Q}_v, A[n])$.

Observation: $L_v \leq H^1(\mathbb{Q}_v, A[n])$ comprises classes that are split by an unr. extn of $\mathbb{Q}_p$.

Galois cohomology $\Rightarrow$ $H^1(G_{\mathbb{Q},S}, A[n])$ of classes in $H^1(\mathbb{Q}, A[n])$ that are unr. at all places outside a fin. set S is fin.

Take $S = \{$places of bad redn, infinite, places dividing $n\}$

For us (setting of Thm B), look at p^n torsion. Take $S = \{N, p, \infty\}$

§2. Translation to étale cohomology

• $\mathcal{A}$ Néron model of A over $\mathbb{Z}$ NMP: $\mathcal{A}(\mathbb{Z}) = A(\mathbb{Q})$

• SES of étale sheaves / $\mathbb{Z}[1/Np]$

$$0 \to \mathcal{A}[p^n] \to \mathcal{A} \xrightarrow{p^n} \mathcal{A} \to 0$$

LES $\Rightarrow$

$$0 \to \frac{\mathcal{A}(\mathbb{Z}[1/Np])}{p^n\mathcal{A}(\mathbb{Z}[1/Np])} \to H^1_{\text{ét}}(\operatorname{Spec}(\mathbb{Z}[1/Np], \mathcal{A}[p^n]) \to H^1_{\text{ét}}(\operatorname{Spec}(\mathbb{Z}[1/Np], \mathcal{A}[p^n])[p^n] \to \cdots$$

NMP $\shortparallel$ $\qquad\qquad$ $\shortparallel$

$A(\mathbb{Q})/p^nA(\mathbb{Q}) \qquad H^1(G_{\mathbb{Q},S}, A[p^n]) \qquad S = \{N, p, \infty\}$

Want to extend to Spec $\mathbb{Z}$.

Problem: $[p^n]: \mathcal{A} \to \mathcal{A}$ not ét. + surj.

Fixes: • take id. component $\mathcal{A}^0$ (throw away non-id component in every fiber – i.e., only at N) ← component gp.

⌈Recall: $0 \to \mathcal{A}^0 \to \mathcal{A} \to \Phi \to 0$ ⌋

But $[p^n]: \mathcal{A}^0 \to \mathcal{A}^0$ is still not surj. of ét. sheaves

• use fppf instead & becomes surj.

Now,

$$0 \to \mathcal{A}^0[p^n] \to \mathcal{A}^0 \to \mathcal{A}^0 \to 0 \quad \text{in fppf}$$

Want to bound $\mathcal{A}^0(\mathbb{Z})/p^n\mathcal{A}^0(\mathbb{Z})$ by $H^1_{\text{ét}}(\operatorname{Spec}\mathbb{Z}, \mathcal{A}^0[p^n])$

Idea:

1) Show that $G_n := \mathcal{A}^0[p^n]$ is admissible

2) Use $h^1(G_n) - h^0(G_n) \leq \delta(G_n) - \alpha(G_n)$

$\ell(G) = \log_p \# G_{\mathbb{Q}}$

$\delta(G) = \log_p(\# G_{\mathbb{Q}}) - \log_p(\# G_{\mathbb{F}_N}\ldots$

$\alpha(G) = \#\, \mathbb{Z}/p\mathbb{Z}$ in the adm. filn. of G

$h^i(G) = \log_p(\# H^i_{\text{ét}}(\operatorname{Spec}\mathbb{Z}, G)\ldots$

§ Checking admissibility

pre-adm. / $\mathbb{Z}[1/N]$: fin. flat, commutative, killed by power of p

$\mathbb{Z}$: comm., sep., fin. presentation, quasi-fin., killed by a power of p; resn to $\mathbb{Z}[1/N]$ is pre-adm.

adm. : pre-adm. + filn. $0 = F^0(G) \subset \cdots \subset F^n(G) = G$. w/ $F^{n+1}G/F^nG \simeq \mathbb{Z}/p\mathbb{Z}$ or μ_p, $\forall n$.

Prop: G pre-adm. gp. sch. / $\mathbb{Z}[1/N]$. Then G is adm. iff $G(\overline{\mathbb{Q}})$ is adm., in the sense that:

A $G_{\mathbb{Q}}$-mod. V is adm if $\exists$ filn w/ each graded piece 1-dim. $\mathbb{F}_p$ v.s. w/ triv. or cyclotomic action.

Pf skh: $F^1V \subset G(\overline{\mathbb{Q}})$ first step of filn (order p). Thm "1.1" from Lec.

$\Rightarrow F^1 V$ ~~is~~ corresponds to some subgp $\tilde{H}_1 \leq G$. closure H_1 in G, order p.

Over $\mathbb{Z}[1/Np]$, H_1 is fin. ét. $\Rightarrow H_1 \simeq \mathbb{Z}/p\mathbb{Z}$ or μ_p. $/\mathbb{Z}[1/Np]$

Raynaud $\Rightarrow$ true over $\mathbb{Z}[1/N]$.

Now, continue by considering G/H_1 & induction. ~~on~~

$\square$

Upshot: $A^\circ[p^n]$ is admissible.

Trick: WLOG, A is self-dual. (Replace A by $A \times A^\vee$)

- $g = \dim A$
- $(G_n)_{\mathbb{F}_{\cancel{p}\,N}} = A^\circ_{\mathbb{F}_N}[p^n]$ (\$p^n\$-torsion of) is an alg. torus $\Rightarrow \log_p(\# G_n(\mathbb{F}_N)) = ng$

$\Rightarrow \ell(G_n) = 2gn$

$\delta(G_n) = 2gn - gn = gn$

α is additive $\Rightarrow \alpha \cancel{\#} (G_n) = n\,\alpha(G_1)$

- ét. $\Rightarrow$ only $\mathbb{Z}/p\mathbb{Z}$ or μ_p
- self-dual $\Rightarrow$ equal number

$\Rightarrow \alpha(G_1) = g.\quad \alpha(G_n) = gn.$

$$\Rightarrow h^1(G_n) - \underbrace{h^0(G_n)}_{\substack{\parallel \\ \log_p(\# A^\circ(\mathbb{Z})[p^n]) \\ \leq \\ A(\mathbb{Z})[p^n] = A(\mathbb{Q})[p^n]}} \leq \delta(G_n) - \alpha(G_n) = 0$$

$A(\mathbb{Z})[p^n] = A(\mathbb{Q})[p^n]$ bdd by Mordell-Weil

$\Rightarrow h^1(G_n)$ bdd indep. of n.

$\Rightarrow A^\circ(\mathbb{Z}) / p^n A^\circ(\mathbb{Z})$ bdd. as $n \to \infty$

But $A^\circ(\mathbb{Z})$ is of fin. index in $A(\mathbb{Z}) \Rightarrow A^\circ(\mathbb{Z})$ fin. gen. $\Rightarrow A^\circ(\mathbb{Z})$ has rk 0. $\square$