Talk on Mochizuki's paper

"Arithmetic elliptic curves in general position"

CMI Workshop in Oxford, December 2015

Ulf Kühn, Universität Hamburg

Overview

abc-conjecture.

Let $\epsilon > 0$, then there exists a $\kappa_\epsilon \in \mathbb{R}$ such that for any coprime $a, b, c \in \mathbb{N}$ with $a + b = c$ we have

$$c \leq \kappa_\epsilon \Big(\prod_{\substack{p \mid abc \\ p \text{ prime}}} p \Big)^{1+\epsilon}.$$

In this talk we report on Mochizuki's work on

Part I: the transfer of the abc-conjecture into an inequality for the height of points in $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and its equivalent refinement for points in compactly bounded subsets of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$.

Part II: a criterion for the surjectivity of the ℓ-adic Galois representation of elliptic curves without complex multiplication given in terms of the Faltings height.

arithmetic degree

K number field with ring of integers $\mathcal{O}_K$.

arithmetic divisor:

$$\sum_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}_K} a_{\mathfrak{p}}\,\mathfrak{p} + \sum_{\sigma:K\hookrightarrow\mathbb{C}} r_\sigma\,\sigma, \qquad a_{\mathfrak{p}}\in\mathbb{Z},\ \ r_\sigma\in\mathbb{R}$$

principal arithmetic divisor:

$$\widehat{\operatorname{div}}(f) := \sum_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}_K} \operatorname{ord}_{\mathfrak{p}}(f)\,\mathfrak{p} + \sum_{\sigma:K\hookrightarrow\mathbb{C}} -\log\|f\|_\sigma\sigma, \qquad f\in K^*$$

arithmetic degree:

$$\widehat{\deg} : \{\text{arith.div.}\}/\{\text{pr.arith.div.}\}\to\mathbb{R}$$

$$\sum_{\mathfrak{p}\in\operatorname{Spec}\mathcal{O}_K} a_{\mathfrak{p}}\,\mathfrak{p} + \sum_{\sigma:K\hookrightarrow\mathbb{C}} r_\sigma\sigma \mapsto \frac{1}{[K:\mathbb{Q}]}\Big(\sum a_{\mathfrak{p}}\log\|\mathfrak{p}\| + \sum_{\sigma:K\hookrightarrow\mathbb{C}} r_\sigma\Big)$$

Arakelov height function

$X_{/K}$ smooth projective curve and L a line bundle on X

$\mathcal{X} \to \operatorname{Spec} \mathcal{O}_K$ regular model for X, i.e. "arithmetic surface"

$\bar{\mathcal{L}} = (\mathcal{L}, \| \cdot \|)$ hermitian line bundle for L on $\mathcal{X}$, i.e. a line bundle with smooth hermitian metric

$P \in X(K)$ determines a section

$$P : \operatorname{Spec} \mathcal{O}_K \to \mathcal{X}$$

height function w.r.t. $\bar{\mathcal{L}}$ and $\mathcal{X}$:

$$\begin{aligned} \mathrm{ht}_{\overline{\mathcal{L}}} : \quad X(K) &\to \mathbb{R} \\ P &\mapsto \widehat{\deg}(P^* \overline{\mathcal{L}}\,) \end{aligned}$$

(here $P^*\overline{\mathcal{L}}$ determines via the choice of a section an arithmetic divisor and $\widehat{\deg}$ anihilates the dependence of that choice)

Fact: Other choices for the models $\mathcal{X}, \mathcal{L}$ and $\|\cdot\|$ change the height by a bounded function, i.e. the **bounded discrepancy class** of the height function $\mathrm{ht}_{\overline{\mathcal{L}}}$ is well-defined.

Proposition(Northcott+ϵ)

Let L be an ample line bundle on X. For any $c \in \mathbb{R}$ we have

$$\sharp\left\{P \in X(\overline{\mathbb{Q}}) \,\middle|\, [K(P):\mathbb{Q}] = d,\ \mathrm{ht}_{\bar{\mathcal{L}}}(P) < c\right\} < \infty.$$

Example. Take $X = \mathbb{P}^1$, $\bar{\mathcal{L}} = (\mathcal{O}(1), \|\cdot\|_{F.S.})$ and $P = [r:s] \in \mathbb{P}^1(\mathbb{Q})$ with coprime $r, s \in \mathbb{Z}$, then we have

$$\mathrm{ht}_{\bar{\mathcal{L}}}(P) = \log\left(\sqrt{|r|^2 + |s|^2}\right).$$

Observe

$$\log\left(\max(|r|, |s|)\right) \leq \mathrm{ht}_{\bar{\mathcal{L}}}(P).$$

log different, log conductor

logarithmic discriminant: $P \in X(\overline{\mathbb{Q}})$ has a minimal field of definition $K(P)$, then

$$\text{log-diff}(P) := \frac{1}{[K(P):\mathbb{Q}]} \log \left| D_{K(P)|\mathbb{Q}} \right|$$

logarithmic conductor relative to a divisor $D \subset X$: Choose extensions $\mathcal{X}$ and $\mathcal{D}$, then for $P \in X(K)$ it is given by

$$\text{log-cond}_D(P) := \widehat{\deg}((P^*\mathcal{D})_{\mathrm{red}})$$

Observe that, in both log-diff and log-cond the archimedean primes will not contribute.

Fact: Other choices for $\mathcal{X}$ and $\mathcal{D}$ change log-cond_D by a bounded function.

Example. Take $X = \mathbb{P}^1(\mathbb{Q})$, $D = 0 + 1 + \infty$ and $P = [r : s]$ with coprime $r, s \in \mathbb{Z}$, then its logarithmic conductor w.r.t. D equals

$$\text{log-cond}_D(P) = \sum_{p | r(s-r)s} \log(p).$$

Indeed, a prime number p contributes, if and only if

$$[r : s] \equiv \begin{cases} [0 : 1] & \text{mod } p \quad \text{if} \quad p | r \\ [1 : 1] & \text{mod } p \quad \text{if} \quad p | (s - r) \\ [1 : 0] & \text{mod } p \quad \text{if} \quad p | s \end{cases}$$

uniform abc-conjecture.

On $\mathbb{P}^1(\overline{\mathbb{Q}}) \setminus D$ with $D = 0 + 1 + \infty$ we have for all $\epsilon > 0$ the inequality of bounded discrepancy classes

$$\text{ht}_{\mathcal{O}(1)} \lesssim (1 + \epsilon)\big(\text{log-cond}_D + \text{log-diff}\big).$$

Fact: implies abc-conjecture: take for $a + b = c$ the point $[a : c]$.

abc-conjecture $\Longleftrightarrow$ Vojta's height inequality

$X_{/K}$ smooth, proper, geometrically connected curve

$U_X := X \setminus D$ with $D \subseteq X$ a reduced divisor

ω_X the canonical sheaf on X.

hyperbolic pair: (X, D) s.t. $\deg(\omega_X(D)) > 0$, called trivial if $D = \emptyset$

$U_X(\overline{\mathbb{Q}})^{\leq d} \subseteq U_X(\overline{\mathbb{Q}})$ the subset of $\overline{\mathbb{Q}}$-rational points defined over a finite extension field of $\mathbb{Q}$ of degree $\leq d$, for d a positive integer.

Theorem.(Bombieri, Elkies, Frankenhuysen, Vojta)

The following conjectures are equivalent

1) Uniform abc-conjecture

2) Vojta's height inequality (VHI): For any hyperbolic pair (X, D) and any $\epsilon > 0$ we have on $U_X(\overline{\mathbb{Q}})^{\leq d}$ the inequality of bounded discrepancy classes

$$\mathrm{ht}_{\omega_X(D)} \lesssim (1+\epsilon)\big(\, \text{log-cond}_D + \text{log-diff}\,\big)$$

Proof: 2) $\Rightarrow$ 1): just take the hyperbolic pair $(\mathbb{P}^1, 0+1+\infty)$

1) $\Rightarrow$ 2): need two steps
first step: abc $\Rightarrow$ VHI for trivial hyperbolic pairs
second step: VHI for trivial hyperbolic pairs $\Rightarrow$ VHI

Claim. abc $\Rightarrow$ VHI for trivial hyperbolic pairs.

Proof: Let Y be a hyperbolic curve, $\phi : Y \to \mathbb{P}^1$ a Belyi map and set $E = \phi^{-1}(D)$ with $D = 0 + 1 + \infty$, then $\omega_Y(E) = \phi^*(\omega_{\mathbb{P}^1}(D))$. Well-known functorialies and a generalised Chevalley-Weil theorem

$$\text{log-diff}_{\mathbb{P}^1} + \text{log-cond}_D \lesssim \text{log-diff}_Y + \text{log-cond}_E$$

imply

$$\begin{aligned}
\text{ht}_{\omega_Y} &\underset{\sim}{=} \text{ht}_{\omega_Y(E)} - \text{ht}_E \underset{\sim}{=} \text{ht}_{\mathbb{P}^1(D)} - \text{ht}_E \\
&\lesssim (1+\epsilon)\big(\,\text{log-diff}_{\mathbb{P}^1} + \text{log-cond}_D\,\big) - \text{ht}_E \qquad (abc) \\
&\lesssim (1+\epsilon)\big(\,\text{log-diff}_Y + \text{log-cond}_E\,\big) - \text{ht}_E \\
&\lesssim (1+\epsilon)\big(\,\text{log-diff}_Y + \text{ht}_E\big) - \text{ht}_E \\
&\lesssim (1+\delta)\,\text{log-diff}_Y
\end{aligned}$$

in the last step we replaced ht_E by a multiple of ht_{ω_Y}. $\square$

Claim. VHI for trivial hyperbolic pairs $\Rightarrow$ VHI.

Proof. Let (X, D) be a hyperbolic pair and choose $\phi : Y \to X$ to be a Galois cover, s.t. Y is hyperbolic, ϕ is etale over $X \setminus D$ and the ramification index equals a "large" p at each point of ramification. Then using well-known functorialities and a generalised Chevalley-Weil theorem

$$\begin{aligned} \mathrm{ht}_{\omega_X(D)} &\lesssim (1+\delta)\,\mathrm{ht}_{\omega_Y} && \text{"large"} \\ &\lesssim (1+\delta)^2 \,\text{log-diff}_Y && (VHI) \\ &\lesssim (1+\delta)^2 \big(\,\text{log-diff}_X + \text{log-cond}_D\,\big) \end{aligned}$$

Finally we replace $(1+\delta)^2$ by $1+\epsilon$. $\square$

Mochizuki: abc-conjecture for compactly bounded subsets

$X_{/\mathbb{Q}}$ smooth projective curve

$V \subset \mathbb{V}(\mathbb{Q})$ a finite subset of absolute values including the archimedean absolute values. For each $v \in V$ choose $\iota_v : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_v$.

Assume for each $v \in V$ we have a non-empty $\mathrm{Gal}(\overline{\mathbb{Q}}_v|\mathbb{Q}_v)$-stable subset $\mathcal{K}_v \subsetneq X(\overline{\mathbb{Q}}_v)$, s.t. for every finite extension $K|\mathbb{Q}_v$, the set $\mathcal{K}_v \cap X(K)$ is a compact domain.

Definition

With the above data a compactly bounded subset is defined as

$$\mathcal{K}_V := \bigcup_{[L:\mathbb{Q}]<\infty} \left\{ x \in X(L) \,\middle|\, \forall \sigma \in \mathrm{Gal}(L|\mathbb{Q}) \,:\, \iota_v(x^\sigma) \in \mathcal{K}_v,\ \forall v \in V \right\}.$$

Observe $\mathcal{K}_V \subset X(\overline{\mathbb{Q}})$.

Theorem. (Mochizuki)

The following conjectures are equivalent:

1) Vojta's height inequality holds for hyperbolic pairs.

2) For compactly bounded subsets of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ the abc-conjecture holds.

Proof: 1)$\Rightarrow$2): easy, VHI $\Rightarrow$ abc $\Rightarrow$ abc for compactly bounded subsets.
2)$\Rightarrow$1): follows by contradiction using the following application of non-critical Belyi maps.

Lemma.

Let Σ be a finite set of prime numbers, Y a hyperbolic curve such that for some $\delta > 0$ the inequality $\mathrm{ht}_{\omega_Y} \lesssim (1+\delta)\,\text{log-diff}_Y$ is false on $Y(\overline{\mathbb{Q}})^{\leq d'}$ for some $d' \in \mathbb{N}$. Then there exists

(i) a positive integer $d \in \mathbb{N}$ and a sequence $(\xi_n)_{n\in\mathbb{N}}$, whose underlying set Ξ is contained in $Y(\overline{\mathbb{Q}})^d$ such that

$$\lim_{n\to\infty} \left| \mathrm{ht}_{\omega_Y}(\xi_n) - (1+\delta)\cdot \text{log-diff}_Y(\xi_n) \right| = \infty$$

i.e. the Vojta height inequality is false on Ξ.

(ii) a Belyi map $\phi : Y \to \mathbb{P}^1$, non-critical at the points of Ξ

(iii) a compactly bounded subset $K_V \subset \mathbb{P}^1 \setminus \{0,1,\infty\}$, whose support contains Σ, such that

$$\phi(\Xi) \subset K_V \bigcap \left(\mathbb{P}^1 \setminus \{0,1,\infty\}(\overline{\mathbb{Q}})\right)^{\leq d}.$$

Proof: i) is clear
ii) + iii) Idea: w.l.o.g. the sequence ξ_n has finitely many v-adic accumulation point. Now, since further technical conditions are satisfied, there is a non-critical Belyi map, i.e. $\phi(\Xi) \not\supset \{0,1,\infty\}$, whose image is contained in a compactly bounded subset. $\square$

If we consider $\mathbb{P}^1 \setminus \{0,1,\infty\}$ via the Legendre family as the moduli of elliptic curves with rational 2-torsion, then the abc-conjecture for compactly bounded subsets is nothing else than a variant of the Szpiro conjecture.

Szpiro conjecture on compactly bounded subsets.

Let $\big(E,\Gamma(2)\big)_{/K}$ be a semi-stable elliptic curve with K-rational 2-torsion that is contained in $\mathcal{K}_V$, then

$$\frac{1}{6}\log|\Delta_E| \lesssim (1+\varepsilon)\big(\text{log-diff}(K) + \text{log-cond}(E)\big).$$

Indeed we just used that on any compactly bounded subset $\mathcal{K}_V$ we have $\frac{1}{6}\log|\Delta_E| \eqsim \mathrm{ht}_\infty(E)$. The bounded functions may depend on $\mathcal{K}_V$.

Resume on part I of this talk

– The techniques to prove all the results so far are standard.

– "VHI $\Longleftrightarrow$ abc conjecture", was known before. The consequent use of the generalised Chevalley-Weil theorem significantly improved the presentation of proof.

– The idea to study the abc-conjecture for compactly bounded subsets is new. The notion non-critical Belyi map is due to Mochizuki.

– additional references:
Bombieri-Gubler: Heights in Diophantine Geometry
Vojta: Diophantine Approximations and Value distributions
Matthes: Master thesis, Hamburg 2013

Motivation for part II

Full Galois action

Let $E_{/K}$ be an elliptic curve without complex multiplication and consider its ℓ-adic Galois representation

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}|K) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell).$$

1) (Serre) There exists ℓ_0 s.t. ρ_ℓ is surjective for all $\ell > \ell_0$.

2) (Masser-Wüstholz, ..., Le Fourn) If $\ell \nmid D_{K|\mathbb{Q}}$ and

$$\ell > 10^7[K:\mathbb{Q}]^2\Big(\max(\mathrm{ht}_{\mathrm{Fal}}(E), 985) + 4\log[K:\mathbb{Q}]\Big)^2,$$

then ρ_ℓ is surjective.

3) (Mochizuki) There is an explicit constant C_ϵ s.t., if

$$\ell > 23040 \cdot 100 \cdot [K:\mathbb{Q}]\Big(\mathrm{ht}_{\mathrm{Fal}}(E) + C_\epsilon + [K:\mathbb{Q}]^\epsilon\Big),$$

$\ell \nmid D_{K|\mathbb{Q}}$ and if $\mathrm{SL}_2(\mathbb{Z}_\ell) \not\subseteq \mathrm{Im}(\rho_\ell)$, then E belongs to finite set.

Elliptic curves

$E_{/K}$ elliptic curve over a number field K

For each $\sigma : K \hookrightarrow \mathbb{C}$ we have

$$E_\sigma(\mathbb{C}) \cong \mathbb{C}/\big(\mathbb{Z} + \mathbb{Z}\tau_\sigma\big) \cong \mathbb{C}^*/q_\sigma^{\mathbb{Z}},$$

where $\mathrm{Im}(\tau_\sigma) > 0$ and $q_\sigma = \exp(2\pi i \tau_\sigma)$.

After replacing K by a finite extension we can assume that E has semi-stable reduction, i.e. for each $\mathfrak{p} \in \mathcal{O}_K$ the reduction of E is either an elliptic curve or a node.

$\mathcal{M}_{Ell}$ moduli space of semi-stable elliptic curves (if possible we supress that it is a stack). We have

$$\mathcal{M}_{Ell}(\mathbb{C}) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \cup \{\infty\} = \mathbb{P}^1(\mathbb{C}).$$

$\underline{\omega}_E := e^*\Omega_{\mathcal{E}/\mathcal{M}_{Ell}}$ Hodge bundle, i.e. the modular form bundle since

$$\underline{\omega}_E^{12} \cong \mathcal{O}(\infty).$$

The fiberwise flat metric $\|\cdot\|$ on $\underline{\omega}_E$ given by integration has a logarithmic singularity at the cusp ∞.

Faltings height

Faltings height is the logarithmically singular height function given by

$$\begin{aligned} \mathrm{ht}_{Fal} :\ \mathcal{M}_{Ell} &\to \mathbb{R} \\ E &\mapsto \widehat{\deg}\left(E^*(\underline{\omega}_E, \|\cdot\|) \right). \end{aligned}$$

One shows that

$$\mathrm{ht}_{Fal}(E) = \frac{1}{[K:\mathbb{Q}]} \cdot \left(\log\left|\Delta_E^{min}\right| - \sum_{\sigma: K \hookrightarrow \mathbb{C}} \log \|\Delta(\tau_\sigma)\|_{Pet}^{1/12} \right),$$

where Δ_E^{min} is the minimal discriminant of E and $\Delta(\tau)$ is the modular discriminant function.

Comparison.

We have with the abreviation $\mathrm{ht}_\infty = \mathrm{ht}_{\mathcal{O}_{\mathcal{M}_{Ell}}(\infty)}$,

$$\mathrm{ht}_\infty(E) \lesssim 12 \cdot (1+\epsilon)\, \mathrm{ht}_{\mathrm{Fal}}(E) \lesssim (1+\epsilon)\, \mathrm{ht}_\infty(E)$$

Proof: Follows from $12 \cdot \mathrm{ht}_{Fal} \lesssim \mathrm{ht}_\infty(E) - \log\left(\mathrm{ht}_\infty(E) \right)$ $\square$

For the following we scale the metrics such that we have

$$\widehat{\deg}(\infty^* E) = \frac{1}{[K:\mathbb{Q}]}(E,\infty)_{\mathrm{fin}} \leq \mathrm{ht}_\infty(E)$$

and such that with a positive constant $C_\infty \in \mathbb{R}$

$$\mathrm{ht}_\infty \leq 13 \cdot \big(\mathrm{ht}_{\mathrm{Fal}} + C_\infty\big).$$

Proposition.

Let $\phi : A \to B$ be an isogeny of elliptic curves, then

$$\mathrm{ht}_{\mathrm{Fal}}(B) \leq \mathrm{ht}_{\mathrm{Fal}}(A) + \frac{1}{2}\log(\deg(\phi)).$$

Proof: Ignore the finite contributions in the general formula

$$\mathrm{ht}_{\mathrm{Fal}}(B) - \mathrm{ht}_{\mathrm{Fal}}(A) = \text{"finite contributions"} + \text{"metric contributions"}.$$

$\square$

Tate curve

Near the cusp ∞ the universal elliptic curve $\mathcal{E}$ over $\mathcal{M}_{Ell}$ is described by the Tate curve:

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

with explicit power series $a_4, a_6 \in q\,\mathbb{Z}[[q]]$ and q a local coordinate.

Let K be a local field and let $q \in K^*$ with $0 < |q| < 1$. Then the analytic torus $K^*/q^{\mathbb{Z}}$ is isomorphic to the elliptic curve given by the Tate curve E_q.

Theorem.

Let E be an elliptic curve over a local field K. After finite extension of the ground field there are two possibilities:

(a) If $|j(E)| \leq 1$, then E has good reduction.

(b) If $|j(E)| > 1$, then E is isomorphic to $K^*/q^{\mathbb{Z}}$ for a unique $q \in K^*$ with $0 < |q| < 1$. The j-invariant bijectively depends on q by $j(q) = \frac{1}{q} + f(q)$ with a power series $f(q) \in \mathbb{Z}[[q]]$.

Relating Galois theory to heights

Crucial observation

Let $E_{/K} \cong K^*/q^{\mathbb{Z}}$ be an elliptic curve curve with $|j(E)| > 1$ over a p-adic field K with normalised valuation ord_v, then $\mathrm{ord}_v(q)$ equals the intersection multiplicity of $E_{/R}$ with $\infty_{/R}$ in the arithmetic surface $\mathcal{M}_{Ell,R}$ over the valuation ring R of K, i.e. the local height of E in the sense of Mochizuki

Let K be a p-adic field with normalized valuation ord_v, let $E_{/K}$ be an elliptic curve with $|j(E)| = 1/|q| > 1$, and let $\ell > 3$ be a prime not dividing $\mathrm{ord}_v(q)$. Then there is an element σ in the inertia subgroup of $\mathrm{Gal}(\bar{K}|K)$ which acts on the ℓ-torsion subgroup $E[\ell]$ of E via a matrix of the form $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. In other words, there is a basis $P_1, P_2 \in E[\ell]$ s. t.

$$\sigma(P_1) = P_1 + P_2 \quad \text{and} \quad \sigma(P_2) = P_2.$$

Proof: Use the description $E_{/\bar{K}}[\ell] = \langle \zeta_\ell, q^{\frac{1}{\ell}} \rangle$. $\square$

Lemma. (rational $\Gamma_0(\ell)$-structure)

Let $E_{/K}$ be a semi-stable elliptic curve over a number field K and let ℓ be a prime, which is prime to all local heights of E. If E has a $\Gamma_0(\ell)$-structure, i.e. a $K-$rational subgroup $H \cong \mathbb{Z}/\ell\mathbb{Z}$, then there exist a positive constant $C_\infty \in \mathbb{R}$ s.t.

$$\ell \,\widehat{\deg}(\infty^* E) \leq 13\big(\,\mathrm{ht}_{\mathrm{Fal}}(E) + \frac{1}{2}\log(\ell) + C_\infty\big). \tag{1}$$

Proof: Apply the height inequality

$$\widehat{\deg}(\infty^* E') \leq 13\big(\,\mathrm{ht}_{\mathrm{Fal}}(E') + C_\infty\big)$$

to the elliptic curve $E' = E/H$. The claim follows since at each prime of bad reduction $E' \cong E_{q'}$ with $q' = q^\ell$ and therefore

$$\widehat{\deg}(\infty^* E') = \ell \,\widehat{\deg}(\infty^* E)$$

and since the isogeny $E \to E/H$ has degree $|H| = \ell$

$$\mathrm{ht}_{\mathrm{Fal}}(E') = \mathrm{ht}_{\mathrm{Fal}}(E) + \frac{1}{2}\log(\ell)$$

$\square$

Proposition.

Let $E_{/K}$ be a non-CM semi-stable elliptic curve over a number field K with $d = [K : \mathbb{Q}]$. Let ℓ be a prime such that

$$\ell > \frac{2d}{\log(2)}\Big(14\,\mathrm{ht}_{\mathrm{Fal}}(E) + 13\log(d) + 13C_\infty\Big). \qquad (2)$$

If E has a $\Gamma_0(\ell)$-structure, then E belongs to a Galois-finite subset of $\mathcal{M}_{\mathrm{ell}}(\overline{\mathbb{Q}})$.

Proof. Let v be the local height at a prime of bad reduction, then

$$v\frac{\log(2)}{d} \leq \widehat{\deg}(\infty^* E) \leq 13\big(\,\mathrm{ht}_{\mathrm{Fal}}(E) + C_\infty\big).$$

i.e.

$$v \leq \frac{13d}{\log(2)}\big(\,\mathrm{ht}_{\mathrm{Fal}}(E) + C_\infty\big) < \ell.$$

Thus ℓ is coprime to all the local heights and the Lemma applies.

With $\log(x) \leq ax - \log(a) - 1$ (different to Mochizuki) we then get

$$\begin{aligned}
\ell \frac{\log(2)}{d} &\leq \widehat{\deg}(\infty^* E_H) \\
&\leq 13 \cdot \Big(\mathrm{ht}_{\mathrm{Fal}}(E) + \frac{1}{2} \log(\ell) + C_\infty \Big) \\
&\leq 13 \cdot \Big(\mathrm{ht}_{\mathrm{Fal}}(E) + \frac{1}{2} \frac{\log(2)}{13d} \ell + \log\Big(\frac{13}{\log(2)}\, d \Big) - 1 + C_\infty \Big).
\end{aligned}$$

Thus we get

$$\ell \frac{\log(2)}{2d} \leq 13 \cdot \big(\mathrm{ht}_{\mathrm{Fal}}(E) + \log(d) + \log(13/\log(2)) - 1 + C_\infty \big)$$

Replacing ℓ using assumption (2) we further derive

$$\mathrm{ht}_{\mathrm{Fal}}(E) \leq 13 \cdot \big(\log(13/\log(2)) - 1 \big) < 38,$$

which can only hold for finitely many elliptic curves. $\square$

Remark. Mochizuki gets a similar lower bound for ℓ which contains d^ϵ instead of $\log(d)$.

Mochizuki Theorem 3.8 (a)

Theorem (Full special linear Galois action)

Let L be a number field and $d = [L : \mathbb{Q}]$. Let $E_{/L}$ be an elliptic curve without complex multiplication. Let $\epsilon > 0$ and with some constant $C \in \mathbb{R}$ as before we let ℓ be a prime with

$$l \geq 23040 \cdot 100d\big(\mathrm{ht}_{Fal} + C + d^{\epsilon}\big).$$

If the image of the Galois representation

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}|L) \to \mathrm{Gl}_2(\mathbb{Z}_\ell)$$

does not contain $\mathrm{SL}_2(\mathbb{Z}_\ell)$, then E belongs to a finite set.

Proof: For allmost all such ℓ the elliptic curve has no $\Gamma_0(\ell)$ structure, thus the Galois representation is irreducible. Since ℓ is prime to the local heights, it must contain the transvection $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, hence it must be the special linear group. (The factor 23040 eliminates some problems in 3 and 5.) $\square$

Mochizuki Theorem 3.8 (b)

Theorem (Full special linear Galois action on compactly bounded subsets)

Let L be a number field and $d = [L : \mathbb{Q}]$. Let $\mathcal{K}_V \subset \mathcal{M}_{Ell}$ be a compactly bounded subset. Let $E_{/L} \in \mathcal{K}_V$ be an elliptic curve without complex multiplication. Let ℓ be a prime which is coprime to all the local heights of E as well as to $2 \cdot 3 \cdot 5$. If the image of the Galois representation

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}|L) \to \mathrm{Gl}_2(\mathbb{Z}_\ell)$$

does not contain $\mathrm{SL}_2(\mathbb{Z}_\ell)$, then E belongs to a finite set.

Proof: Analogous as before one shows: If $E_{/K}$ has a $\Gamma_0(\ell) -$ *structure* for a prime ℓ which is coprime to all the local heights, then E belongs to finite set. In fact, since we can neglect the archimedean contribution it is even simpler.

□

Mochizuki Corollary 4.3

Corollary. (Full Galois Actions for Degenerating Elliptic Curves)

Let $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$; $\epsilon \in \mathbb{R}_{>0}$. Then there exists a constant $C \in \mathbb{R}_{>0}$ and a Galois-finite subset $\mathfrak{E} \subseteq \mathcal{M}_{Ell}$ which satisfy the following property:
Let $E_{/L}$ be an elliptic curve over a number field $L \subset \mathbb{Q}$, where L is a minimal field of definition of the point $[E_{/L}] \in \mathcal{M}_{Ell}(\overline{\mathbb{Q}})$, and $[E_{/L}] \notin \mathfrak{E}$; S a finite set of prime numbers. Suppose that $E_{/L}$ has at least one prime of potentially multiplicative reduction. Write $d = [L : \mathbb{Q}]$; $x_S \stackrel{\mathrm{def}}{=} \sum p \in S \log(p)$. Then there exist prime numbers $\ell_\circ$, $\ell_\bullet \notin S$ which satisfy the following conditions:

(a) $\ell_\circ$, $\ell_\bullet$ are prime to the primes of potentially multiplicative reduction, as well as to the local heights, of $E_{/L}$. Moreover, $\ell_\bullet$ is prime to the primes of $\mathbb{Q}$ that ramify in L, as well as to the ramification indices of primes of $\mathbb{Q}$ in L.

(b) The image of the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}|L) \to \mathrm{GL}_2(\mathbb{Z}_{\ell_\circ})$ associated to $E_{/L}$ contains $\mathrm{SL}_2(\mathbb{Z}_{\ell_\circ})$. The Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}|L) \to \mathrm{GL}_2(\mathbb{Z}_{\ell_\bullet})$ associated to $E_{/L}$ is surjective.

(c) The inequalities

$$\ell_\circ \leq 23040 \cdot 900d \cdot \mathrm{ht}_{Fal}([E_{/L}]) + 2x_S + C \cdot d^{1+\epsilon}$$

$$\ell_\bullet \leq 23040 \cdot 900d \cdot htf_{Fal}([E_{/L}]) + 6d \cdot \text{log-diff}_{\mathcal{M}_{Ell}}([E_{/L}])) + 2x_S + C \cdot d^{1+\epsilon}$$

hold.

Mochizuki Corollary 4.4

Corollary (Full Galois Actions for Compactly Bounded Subsets)

Let $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$; $\mathcal{K}_V \subseteq \mathcal{M}_{Ell}(\overline{\mathbb{Q}})$ a compactly bounded subset.Then there exists a constant $C \in \mathbb{R}_{>0}$ and a Galois-finite subset $\mathfrak{E} \subseteq \mathcal{M}_{Ell}$ which satisfy the following property:
Let $E_{/L}$ be an elliptic curve over a number field $L \subset \overline{\mathbb{Q}}$, where L is a minimal field of definition of the point $[E_{/L}] \in \mathcal{M}_{Ell}(\overline{\mathbb{Q}})$, and $[E_{/L}] \notin \mathfrak{E}$; S a finite set of prime numbers. Write $d = [L : \mathbb{Q}]$; $x_S \stackrel{\text{def}}{=} \sum p \in S \log(p)$.
Then there exist prime numbers $\ell_\circ$, $\ell_\bullet \notin S$ which satisfy the following conditions:

(a) $\ell_\circ$, $\ell_\bullet$ are prime to the primes of potentially multiplicative reduction, as well as to the local heights, of $E_{/L}$. Moreover, $\ell_\bullet$ is prime to the primes of $\mathbb{Q}$ that ramify in L, as well as to the ramification indices of primes of $\mathbb{Q}$ in L.

(b) The image of the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}|L) \to \mathrm{GL}_2(\mathbb{Z}_{\ell_\circ})$ associated to $E_{/L}$ contains $\mathrm{SL}_2(\mathbb{Z}_{\ell_\circ})$. The Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}|L) \to \mathrm{GL}_2(\mathbb{Z}_{\ell_\bullet})$ associated to $E_{/L}$ is surjective.

(c) The inequalities

$$\ell_\circ \leq 23040 \cdot 100d \cdot \mathrm{ht}_{Fal}([E_{/L}]) + 2x_S + C \cdot d$$

$$\ell_\bullet \leq 23040 \cdot 100d \cdot \mathrm{ht}_{Fal}([E_{/L}]) + 6d \cdot \text{log-diff}_{\mathcal{M}_{Ell}} + 2x_S + C \cdot d$$

hold.

Resume on Part II of this talk

– The techniques to prove all the results so far are standard.

References:

Cornell-Silverman: Arithmetic geometry
Serre: Abelian ℓ-adic Representations and Elliptic Curves
Silverman: Advanced topics on elliptic curves