Notes on the ε part in the *abc* conjecture

(Including Siegel zeros and effectivity in IUT)

Vesselin Dimitrov

July 25, 2016

The *abc* conjecture (*Some notation.*)

On $P \in \mathbb{P}^1(\bar{\mathbb{Q}}) \setminus \{0, 1, \infty\}$*, all* $\varepsilon > 0$ *satisfy*

$$h(P) \leq (1+\varepsilon)\big(\mathrm{cond}_{[0]+[1]+[\infty]}(P) + d(P)\big) + O_{\varepsilon,(\ldots[\mathbb{Q}(P):\mathbb{Q}]?)}(1),$$

where: $h =$ abs. logarithmic Weil height, $d(P) =$ abs. logarithmic root discriminant of the field $\mathbb{Q}(P)$,

$$\mathrm{cond}_{[0]+[1]+[\infty]}(P) := \frac{1}{[\mathbb{Q}(P):\mathbb{Q}]} \sum_v \log|k(v)|$$

over all $v \in M^{\mathrm{fin}}_{\mathbb{Q}(P)}$ having $v(x) > 0, v(1/x) > 0$ or $v(x-1) > 0$ (where $P = [x:1]$).

The *abc* conjecture (A comparison.)

In the case of complex function fields, McQuillan, Yamanoi and Chen have proved Vojta's "$1 + \varepsilon$" conjecture, that the analogous bound holds in $\mathbb{P}^1_B \setminus D$ for D/B any (not necessarily isotrivial) divisor of rel. degree 3. This holds without a dependence on the degree.

The *abc* conjecture (A comparison.)

In the case of complex function fields, McQuillan, Yamanoi and Chen have proved Vojta's "$1 + \varepsilon$" conjecture, that the analogous bound holds in $\mathbb{P}^1_B \setminus D$ for D/B any (not necessarily isotrivial) divisor of rel. degree 3. This holds without a dependence on the degree.

A question: What then is the structure of the error term, in both inequalities? Should we expect the complex function field Vojta conjectures to hold with an $O(1/\varepsilon)$, as is the expectation in the arithmetic case, and that this would be essentially optimal?

The *abc* conjecture, in a form suggested by IUT.

$$\log \Theta \leq \frac{1}{l} \log \mathfrak{q} \quad ?$$

The *abc* conjecture, in a form suggested by IUT.

$$\log \Theta \leq \frac{1}{l} \log \mathfrak{q} \quad ?$$

Let E/F be an elliptic curve, $l \geq 5$ a prime level;
$K = F(E[l])$;

The *abc* conjecture, in a form suggested by IUT.

$$\log \Theta \leq \frac{1}{l} \log \mathfrak{q} \quad ?$$

Let E/F be an elliptic curve, $l \geq 5$ a prime level; $K = F(E[l])$; $h(E/F)$ the Faltings height of E over F; e the highest ramification index in $F/\mathbb{Q}$. Observe that [IUT-IV, 1.10] bounds e by $[F : \mathbb{Q}]$.

The *abc* conjecture, in a form suggested by IUT.

$$(abc_{\ominus}) \qquad 2h(E/F)$$

The *abc* conjecture, in a form suggested by IUT.

$$(abc_{\Theta}) \qquad 2h(E/F) \quad \leq \quad \frac{e}{l} \cdot 2h(E/F)$$

The *abc* conjecture, in a form suggested by IUT.

$$(abc_\Theta) \qquad 2h(E/F) \quad \leq \quad \frac{e}{l} \cdot 2h(E/F) + \frac{1}{[K:\mathbb{Q}]} \log |D_{K/\mathbb{Q}}|$$

The *abc* conjecture, in a form suggested by IUT.

$$(abc_\Theta) \qquad 2h(E/F) \quad \leq \quad \frac{e}{l} \cdot 2h(E/F) + \frac{1}{[K:\mathbb{Q}]} \log |D_{K/\mathbb{Q}}| + E_{\mathrm{hr}}(K/\mathbb{Q}) + C,$$

where, with $e_{p/K}$ the highest ramification index of p in K,

$$E_{\mathrm{hr}}(K/\mathbb{Q}) = \sum_{\substack{p \in M_\mathbb{Q} \\ e_{p/K} \geq p-1}} \log e_{p/K} \quad (\text{“high ramification”}).$$

The *abc* conjecture, in a form suggested by IUT.

In our case (IUT), we have:

$$E_{\mathrm{hr}}(K/\mathbb{Q}) \lesssim \#\{\text{primes } p \leq el \text{ ramifying in } K\} \cdot \log el,$$

which by Chebyshev's theorem is $\ll el$.

The optimal choice of l then gives a square root error term assuming e is bounded, which for example is the case when F ranges through number fields of a fixed degree.

Why would I formulate the *abc* hypothesis like that?

- When $h(E/F)$ is depleted at 2 and ∞, and under the appropriate "genericity" restrictions on initial data (E/F split semistable, K/F a large extension, l prime to the orders of the q-parameters. . .), this is exactly what [IUT-IV, Thm. 1.10] amounts to.

Why would I formulate the *abc* hypothesis like that?

- This is a statement that shows explicitly the role of arithmetic ramification in the structure of the main as well as “error” terms.

Why would I formulate the *abc* hypothesis like that?

- This is a statement that shows explicitly the role of arithmetic ramification in the structure of the main as well as "error" terms.
- It suggests that a similar structure of the error term could be present in generalizations of *abc* (e.g. Vojta's conjectures).

Why would I formulate the *abc* hypothesis like that?

- This is a statement that shows explicitly the role of arithmetic ramification in the structure of the main as well as "error" terms.
- It suggests that a similar structure of the error term could be present in generalizations of *abc* (e.g. Vojta's conjectures).
- It is strong enough to forbid a Landau-Siegel zero at odd Dirichlet characters of $\mathbb{Q}$ (as we shall see in a minute).

Why would I formulate the *abc* hypothesis like that?

- This is a statement that shows explicitly the role of arithmetic ramification in the structure of the main as well as "error" terms.
- It suggests that a similar structure of the error term could be present in generalizations of *abc* (e.g. Vojta's conjectures).
- It is strong enough to forbid a Landau-Siegel zero at odd Dirichlet characters of $\mathbb{Q}$ (as we shall see in a minute).

For this presentation, let me refer to the hypothesis on the previous frame as abc_{Θ}.

Remarks on $X(2l) \to X(2) \cong \mathbb{P}^1$ and on the CM case

(i) This is indeed in the form of a refined Vojta conjecture in the particular case of the complete curve $X(2l)$, which is of hyperbolic type precisely under the $l \geq 5$ assumption.

Remarks on $X(2l) \to X(2) \cong \mathbb{P}^1$ and on the CM case

(ii) $K/\mathbb{Q}$ is always ramified at l, but not wildly ramified when E has CM. In the latter case, as we shall see in a moment, the local discriminant term in abc_Θ imparts just a $\log l + O(1)$. In addition $e_{l/K} = l - 1$ (when l does not ramify in F), so l is included (with equality!) in E_{hr} also.

Remarks on $X(2l) \to X(2) \cong \mathbb{P}^1$ and on the CM case

This gives a $2 \log l$ addition to the main term on the RHS. We shall see that the rest is $O(1)$ for the appropriate field F, and that the resulting inequality is indeed implied by ERH (but is false with coefficient 1 in $\log l$).

Remarks on $X(2l) \to X(2) \cong \mathbb{P}^1$ and on the CM case

This gives a $2 \log l$ addition to the main term on the RHS. We shall see that the rest is $O(1)$ for the appropriate field F, and that the resulting inequality is indeed implied by ERH (but is false with coefficient 1 in $\log l$).

(iii) Here, it is crucial that the E_{hr} term exhibits a sharp jump at $e_{p/K} = p - 1$. One checks that this is indeed a feature of [IUT-IV, Prop. 1.2].

A reformulation on the modular curve (a special case)

The link between the two versions is most naturally made by taking the model $Y(2)$ of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, and noting $2h^{\mathrm{st}}(E) \sim \frac{1}{6}h(j_E) \sim h(\lambda)$.

A reformulation on the modular curve (a special case)

The link between the two versions is most naturally made by taking the model $Y(2)$ of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, and noting $2h^{\mathrm{st}}(E) \sim \frac{1}{6}h(j_E) \sim h(\lambda)$.
Recall $Y(2)_{/\mathbb{C}} = \mathbb{H}/\Gamma(2)$, with $\Gamma(2)$ the kernel of reduction mod 2 in the elliptic modular group $\Gamma(1) = \mathrm{PSL}(2, \mathbb{Z})$. Like any Shimura variety, $Y(2)$ comes with its distinguished "special points," giving elliptic curves with CM. A point $P \in Y(2)(F)$ is represented by an elliptic curve E/F with F-rational 2-torsion and a labeling of its points of order two.

Reformulation on the modular curve: a case of square root error

Let $\mathrm{cond}_{/F}(P) := \frac{1}{[F:\mathbb{Q}]} \log |N_{F/\mathbb{Q}}(\mathfrak{f}_{E/F})|$ the logarithmic conductor and $h_{/F}(P) := h(E/F)$, the Faltings height function. As before, let d_F the logarithmic root discriminant of F. Then $abc_\ominus$ implies a **semi-uniform** *abc* **conjecture**:

$$2h_{/F}(P) \leq \mathrm{cond}_{/F}(P) + d_F$$
$$+O\left(e\sqrt{\mathrm{cond}_{/F}(P) + d_F}\right),$$

(e a bound on the abs, ramification indices of F).

Reformulation on the modular curve: a case of logarithmic error

Furthermore, if E/F has everywhere good reduction then $2h(E/F) \leq d_F + O(e + \log d_F)$ (absolute implied constant).

Reformulation on the modular curve: a case of logarithmic error

Furthermore, if E/F has everywhere good reduction then $2h(E/F) \leq d_F + O(e + \log d_F)$ (absolute implied constant).

Why is this implied by abc_Θ? Well, if E/F has everywhere good reduction then, by Néron-Ogg-Shafarevich, either $p = l$ (with $\log e_{l/K} \ll \log l$), or else $e_{p/K} \leq e$; hence, the E_{hr} term is just $\ll e + \log l$.

Reformulation on the modular curve: a case of logarithmic error

On the other hand, in general,

$$\mathrm{cond}(E/K) + d_K = \mathrm{cond}(E/F) + d_F + O(\log l)$$

See Prop. 1.3 in [IUT-IV], as used in step (ii) on page 24 of *loc.cit.*, or Prop. 14.4.6 (and its proof) in Bombieri and Gubler's *Heights in Diophantine Geometry*.

Now choose $l \sim d_F$ in abc_Θ.

Logarithmic error

The meaning of this is that when the conductor vanishes the error term should be logarithmic, like it is in Nevanlinna's Second Main Theorem.

Special points

What happens at the CM points?

Consider for simplicity (and WLOG) $-D$ a fundamental discriminant and CM points with $\mathrm{End}(E)$ the maximal order O_D in $K_D := \mathbb{Q}(\sqrt{-D})$. Then, by class field theory, E is defined over H_D, the Hilbert class field. H_D/K_D is unramified, hence $d_{H_D} = d_{K_D} = \log \sqrt{D}$. Take F to be the ray class field mod 6 of K_D. It turns out that E extends as an abelian scheme over $\mathrm{Spec}\, O_F$.

An everywhere good reduction model

For classical CM theory gives a model

$$Y^2 = X^3 - 27\gamma_2(\tau)^3 X - 54\gamma_3(\tau)^2$$

for $E_{/\mathbb{C}}$, where $\tau \in K_D$, and γ_2, γ_3 are familiar (Weber's) modular functions for $\Gamma(6)$ satisfying $\gamma_2^3 - \gamma_3^2 = 1728$. Shimura's reciprocity law enforces $\gamma_2(\tau), \gamma_3(\tau) \in O_F$, while the relation shows that this Weierstrass equation has unit discriminant. Now F/H_D is a bounded degree extension of ramification limited to $\{2, 3\}$. Hence, $d_F = \log \sqrt{D} + O(1)$, and $e = O(1)$.

Special points (continued)

Conclusion:
$abc_\Theta \Rightarrow 2h(E/F) \leq \log\sqrt{D} + 2\log\log D + O(1)$.

References: Thm. 5.1.2 in Schertz's *Complex Multiplication*, for Shimura reciprocity; the same book for Weber's functions γ_2, γ_3; and section 2 in Granville and Stark's paper *ABC implies no "Siegel zero"*. . ., that I am presently paraphrasing.

$$2h(E/F) \leq \log \sqrt{D} + 2 \log \log D + O(1)$$

But

$$2h(E/F) = 2h^{\mathrm{st}}_{\mathrm{Fal}}(E) = \log \sqrt{D} + \frac{L'}{L}(1, \chi_D) + O(1),$$

by Kronecker's limit formula!

$$2h(E/F) \leq \log \sqrt{D} + 2 \log \log D + O(1)$$

But

$$2h(E/F) = 2h^{\mathrm{st}}_{\mathrm{Fal}}(E) = \log \sqrt{D} + \frac{L'}{L}(1, \chi_D) + O(1),$$

by Kronecker's limit formula! The right hand side of this formula gives easily an analytic expression of the height, in this CM case, in terms of the zeros of $L(s, \chi_D)$:

$$2h^{\mathrm{st}}(E) = \sum_{\rho} \frac{1}{1-\rho} + O(1) = \sum_{\rho} \mathrm{Re} \frac{1}{\rho} + O(1).$$

The Kronecker limit formula

Here this is averaged over $\mathrm{Pic}(O_D)$, allowing for a purely multiplicative proof, which is elementary given the (logarithmic) equidistribution of the primes of K_D in angular sectors and in ideal classes:

Express both sides, up to $O(1)$, as the average of $\pi y/3 - \log y$ over the dilatations y of the fractional ideals of $\mathbb{Q}(\sqrt{-D}) \subset \mathbb{C}$, and link them via the factorization into prime ideals of the product of all non-zero O_D elements inside a disk of a growing radius (by elaborating on Selberg's proof of Dirichlet's theorem).

$$2h(E/F) \leq \log \sqrt{D} + 2 \log \log D + O(1)$$

Hence, on CM points, our implication of abc_{Θ} amounts exactly to

$$\frac{L'}{L}(1, \chi_D) \leq 2 \log \log D + O(1).$$

$2h(E/F) \leq \log \sqrt{D} + 2 \log \log D + O(1)$

Hence, on CM points, our implication of $abc_{\ominus}$ amounts exactly to

$$\frac{L'}{L}(1, \chi_D) \leq 2 \log \log D + O(1).$$

This is exactly what GRH gives. This upper bound forbids a Landau-Siegel zero for $L(s, \chi_D)$.

Siegel zeros

Indeed, in view of the formula

$$\frac{L'}{L}(1, \chi_D) + \log \sqrt{D} = \sum_{\rho} \frac{1}{1-\rho} + O(1),$$

the no Landau-Siegel zeros conjecture amounts precisely to $\frac{L'}{L}(1, \chi_D) \ll \log D$.

Siegel zeros: implication

This implication is effective if the absolute constant C of abc_{Θ} is effective (as it is in IUT). It would then have as effective consequence an explicit form of the Granville-Stark asymptotic formula for the class number of $\mathbb{Q}(\sqrt{-D})$. It is expected that $\frac{L'}{L}(1, \chi_D) \leq \log\log D + \log\log\log D + O(1)$, known on ERH to be best possible: see [Mourtada M., Murty V.K.: Omega theoremss for $\frac{L'}{L}(1, \chi_D)$, *Int. J. Num. Th.*, vol. **9**, 2013].

Three consequences of this modular point of view, a summary.

(i) The *abc* conjecture is naturally expressed as a bound on the modular height function on $Y(2)$. This is the simplest Shimura variety, suggesting certain extensions of *abc* that *might* not be covered by the Vojta conjectures. (On a related note, Kato has defined a Faltings height for pure motives and has suggested an *abc* conjecture for those heights.)

Three consequences of this modular point of view, a summary.

(ii) Like any Shimura variety, $Y(2)$ is naturally endowed with a collection of special points. On all of these, the conjecture should be an asymptotic equality of a deep analytic number theory significance. E.g., for the Siegel modular variety, Colmez's conjecture (recently proved by Yuan and Zhang in the average over the CM types) suggests a sharp asymptotic bound $1/2 + o(1)$ on the Szpiro ratio $h_{\mathrm{Fal}}(A) / \log N_A$ of *simple* abelian varieties over $\mathbb{Q}$ of a fixed dimension.

Three consequences of this modular point of view, a summary.

(iii) This formulation of abc_{Θ} gives an extremely narrow near-miss at both the Erdös-Stewart-Tijdeman-Masser construction, and on all the CM points.

What could be said from just the $\{2, \infty\}$-depleted form [Thm. 1.10] of abc_Θ?

For $S \subset M_{\mathbb{Q}}$ a finite set of places, let $h^{(S)}$ be the *S-depleted height*, devoid of all components lying over S, and designate as $abc_\Theta^{(S)}$ the corresponding (weaker) hypothesis for this height. As noted before, Thm. 1.10 of [IUT-IV] is essentially $abc_\Theta^{\{2,\infty\}}$.

Reducing to a depleted form

By Mochizuki's "arithmetic analytic continuation via Belyi correspondences" [AECGP], $abc_{\Theta}^{(S)}$ for any S yields the *non-uniform* (degree dependent) form of the *abc* conjecture:

$$abc_{\Theta}^{(S)} \Rightarrow \forall \varepsilon > 0,\ P \in \mathbb{P}^1(\bar{\mathbb{Q}}) \setminus \{0, 1, \infty\},$$
$$h(P) \leq (1+\varepsilon) \cdot (d(P) + \mathrm{cond}_{[0]+[1]+[\infty]}(P)) + O_{\varepsilon, [\mathbb{Q}(P):\mathbb{Q}], |S|}(1).$$

The proof in [AECGP] is phrased as an indirect argument, by contradiction. It turns out that this argument can be made direct and effective.

Effectivity

The following is outlined in the ArXiv preprint [Effectivity]. (Though we shall see that we may sometimes do better, by relaxing Mochizuki's compact boundedness condition.)

Dimitrov V.: Effectivity in Mochizuki's work on the *abc*-conjecture, `ArXiV:1601.03572v1`.

Effectivity

Theorem

There are computable functions $c : \mathbb{N} \times (0,1) \to (0,1)$, $B, C : \mathbb{N} \times (0,1) \times \mathbb{N} \to \mathbb{R}$ *such that the following is true.*

Suppose $A : \mathbb{N} \times (0,1) \to \mathbb{R}$ *is a function such that, for all* d *and* ε, *all* E/F meeting $[F : \mathbb{Q}] \leq d$ and $|j_E|_v \leq B(d, \varepsilon, |S|)$ *for all* $v \in S$ *fulfil* $2h(E/F) \leq (1+\varepsilon)(d_F + \mathrm{cond}(E/F)) + A(d, \varepsilon)$.

Then, *for all* d *and* ε, all E/F *with* $[F : \mathbb{Q}] \leq d$ *fulfil*

$$2h(E/F) \leq (1+\varepsilon)(d_F + \mathrm{cond}(E/F)) \\ +2A(150d\lfloor\varepsilon^{-2}\rfloor, c(d, \varepsilon, |S|)) + C(d, \varepsilon, |S|).$$

Belyi correspondences

The involvement in IUT of the l-division field $K = F(E[l])$ of an elliptic curve, with its attendant constructions like $\underline{\underline{q}} = q^{1/2l}$, makes inherent in the theory one particular Belyi map: the covering $f_l : Y(2l) \to Y(2) \cong \mathbb{P}^1 \setminus \{0, 1, \infty\}$. We could easily formulate a version of abc_Θ for an arbitrary Belyi map f (then the role of l is taken place by the minimum over $f^{-1}\{0, 1, \infty\}$ of the ramification indices of f), but any other choice means giving up the elliptic curve, its theta functions, its associated hyperbolic orbicurves, the fundamental groups and anabelian transport — in short, everything that makes up IUT.

Belyi correspondences: switching dessins

In [AECGP] and in [Effectivity], the dessins are changed not by morphisms but by *correspondences*: diagrams

$$\begin{array}{ccc} & C & \\ {}^{\pi}\swarrow & & \searrow^{f} \\ \mathbb{P}^1 & & \mathbb{P}^1, \end{array}$$

with π, f non-constant morphisms branched only on $\{0, 1, \infty\}$.

Belyi correspondences: switching dessins

$$\begin{array}{ccc} & C & \\ {}^{\pi}\swarrow & & \searrow^{f} \\ \mathbb{P}^1 & & \mathbb{P}^1, \end{array}$$

π should be a basic map having high ramification indices, say $\geq n$, at all points in $\pi^{-1}\{0, 1, \infty\}$. The conceptually simplest choice is the $f_l : Y(2l) \to Y(2)$ above, and from the point of view of equations and computations, the simplest choice is the function x^n on the Fermat curve $C_n : \ x^n + y^n = 1$.

The mechanics of a Belyi correspondence

For any diagram $\pi, f : C \to \mathbb{P}^1$ as before (defined over $\mathbb{Q}$), and any point $P \in \mathbb{P}^1(\bar{\mathbb{Q}})$ of degree d, take a lift $Q \in \pi^{-1}(P)$ and follow $f(Q) \in \mathbb{P}^1(\bar{\mathbb{Q}})$. By Riemann-Hurwitz, with an effective "$O(1)$" in terms of equations for C and π, $h_{K_C}(Q) \geq (1 - 3/n)h(P) + O_\pi(1)$. By a computation of differents using Chevalley-Weil, Riemann-Hurwitz for $E = f^*([0] + [1] + [\infty])_{\mathrm{red}}$ gives. . .

The mechanics of a Belyi correspondence

$$
\begin{aligned}
h_{K_c}(Q) &= h(f(Q)) - h_E(Q) + O_f(1) \\
\leq_{abc} &\ (1+\epsilon)(d(Q) + \mathrm{cond}_E(Q)) - h_E(Q) + O_{\epsilon,f}(1) \\
&\leq (1+\epsilon)d(Q) + \epsilon h_E(Q) + O_{\epsilon,f}(1),
\end{aligned}
$$

if *abc* can be applied to $f(Q)$. The second term is $\ll_{\deg f} \epsilon h_{K_c}(Q)$ and so harmless if $\epsilon \ll_{\deg f} 1$.

“Compact boundedness”

We are left with insuring that *abc* is applicable to $f(Q)$. This follows from $abc_{\Theta}^{\{2,\infty\}}$ — and hence, by additional standard arguments, from Thm. 1.10 of [IUT-IV], — if we arrange for the Galois orbit of $f(Q)$ to be bounded away from the cusps $[0] + [1] + [\infty]$ at the places 2 and ∞.

This is constructive

The Galois orbit has size at most $d \deg \pi$ (view it as a random subset of cardinal $d \deg \pi$ in $\mathbb{P}^1(\bar{\mathbb{Q}})$), so if we just take any $2d \deg \pi + 1$ Belyi maps having pairwise disjoint critical loci, the pigeonhole principle implies that for all choices of P of degree d, the Galois orbit of $Q(\in \pi^{-1}(P))$ will be bounded away from the critical locus of one of these maps, at both places 2 and ∞. Then, at 2 and ∞, the Galois orbit of $f(Q)$ is bounded away from the cusps of $Y(2)$.

This is constructive

Everything is completely effective, and quite easy to follow if we use the Fermat curve $x^l + y^l = 1$*, the map* $\pi = x^l$*, and the standard presentation of a rational function* f *on that curve as a uniquely determined element of*
$\mathbb{Q}(x) + y \cdot \mathbb{Q}(x) + \cdots + y^{l-1} \cdot \mathbb{Q}(x)$.

Disjoint critical loci

Mochizuki proves in [Noncritical Belyi maps] that the Belyi opens form a basis for Zariski topology on any curve. Another proof is presented in [Scherr Z., Zieve M.: Separated Belyi maps, *Math. Res. Lett.*, vol. **21**, 2014]. Both are effective; see also section 2 of [Effective], for the precise meaning of this. Hence we may place a computable, indeed explicit bound $N(l, d)$ for which we can ascertain $2dl^2 + 1$ Belyi maps on $x^l + y^l = 1$ having pairwise disjoint critical loci, and such that all polynomials involved in the presentations these Belyi maps have degrees and heights less than $N(l, d)$.

Effective, but inefficient

The problem with this algorithmic procedure is that it is terribly inefficient, due to the successive compositions in Belyi's algorithm that are needed to reduce critical values from $\bar{\mathbb{Q}}$ to $\mathbb{Q}$. These make even the constant $N(4,1)$, which is the smallest non-trivial case, gigantic — on the order of 40! (forty factorial). Note that this is a bound on *logarithmic* heights. May we do better?

Effective, but inefficient

The problem with this algorithmic procedure is that it is terribly inefficient, due to the successive compositions in Belyi's algorithm that are needed to reduce critical values from $\bar{\mathbb{Q}}$ to $\mathbb{Q}$. These make even the constant $N(4, 1)$, which is the smallest non-trivial case, gigantic — on the order of 40! (forty factorial). Note that this is a bound on *logarithmic* heights. May we do better?

(Anyway this is not of much interest at the present stage. Effectivity is interesting as a theoretical point, for the proofs of Roth's and Faltings's theorems are inherently ineffective.)

Relaxing the boundedness condition

This is not clear to me if we insist on bounding *all* the local heights at 2 and ∞ (attaining, that is, compact boundedness). The compact boundedness condition is much too expensive, for the set of all Belyi covers (being in correspondence with the open subgroups of the fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$) has a strong finiteness property for bounded degree, making it clear that the degrees of our requisite maps *must* be somewhat large (and must go to infinity as we need arbitrarily many maps to reach the $1 + \varepsilon$ exponent and higher degree points).

Relaxing the boundedness condition

However, all that is needed from "compact boundedness" is that the 2- and ∞-portions of the height $h(E/F)$ are negligibly small in comparison with the global height $h(E/F)$. In certain situations, as we shall exploit next for large degree d, this is much easier to arrange.

Siegel zeros, from $abc_{\Theta}^{(S)}$

We have seen already that IUT implies effective Roth and Faltings theorems. Let me focus here only on the remaining most significant theoretical implication. As we have seen, hypothesis abc_{Θ} forbids Siegel zeros at odd characters of $\mathbb{Q}$. Does that persist with abc_{Θ}^{S} and IUT?

Siegel zeros, from $abc_{\Theta}^{(S)}$

The answer, after all, is positive.

Theorem

[*IUT-III Cor. 3.12*] *implies an effective* $C < \infty$ *such that* $\frac{L'}{L}(1, \chi) < C \log q$ *for all odd Dirichlet characters* $\chi \mod q$*. In other words, IUT theory forbids a Landau-Siegel zero at the odd Dirichlet characters of* $\mathbb{Q}$*, in an effective manner (giving an effective Siegel theorem for quadratic imaginary fields).*

Preparation for the proof: Habegger's theorem

In a recent paper

> Habegger P.: Singular moduli that are algebraic units, *Algebra and Number Theory*, vol. **9**, no. 7 (2015), pp. 1515–1524,

Philip Habegger obtained a modular analog of Siegel's finiteness theorem on integral points: *For any algebraic $\alpha \in \bar{\mathbb{Q}}$, there are only finitely many CM elliptic curves $E/\bar{\mathbb{Q}}$ such that $1/(j_E - \alpha) \in \bar{\mathbb{Z}}$ is an algebraic integer.*

Habegger's modular Siegel theorem

His proof has two main ingredients: Duke's ineffective hyperbolic equidistribution of CM points on the modular surface $\mathbb{H}/\Gamma(2)$ (which we shall not require), and an effective diophantine approximations result with two elliptic logarithms. The former shows that not too many conjugates of j_E lie near α, and the latter, that none of these conjugates is *too* close to α. The second of these will suffice for us, and we shall apply it in exactly the same way as in Habegger's paper.

Linear forms in two elliptic logarithms

We will use the diophantine approximations result of David and Hirata-Kohno, in exactly the same way that it is used by Habegger (see Lemma 6 there):
Let v be a place of $\bar{\mathbb{Q}}$ and α any fixed algebraic point. Then all conjugates $j(\tau)$ of j_E (assuming $j(\tau) \neq \alpha$) satisfy

$$-\log |j(\tau) - \alpha|_v \leq c(\alpha) \log D,$$

where $c(\alpha)$ depends effectively on $\deg \alpha$ *and $h(\alpha)$.*

Linear forms in two elliptic logarithms

The paper of David and Hirata-Kohno is [*Linear forms in elliptic logarithms*, J. Reine angew. Math. **628** (2009), pp. 37–89]. This is applied to the periods of the elliptic curve of invariant $\alpha \in \bar{\mathbb{Q}}$, using that τ is algebraic (a quadratic integer). Here the CM hypothesis is used crucially.
The relevant portions of [Habegger] here are Lemma 3, Lemma 6 and the calculation in the penultimate paragraph of the paper.

A dessin switch

We shall work on the modular covering $Y(10) \to Y(2)$, so that we have ramification indices ≥ 4 at all three cusps (meaning we may take $n = 4$ in our previous discussion).

We have one Belyi map $\pi = f_{10} : X(10) \to X(2)$. Construct a second one $\psi : X(10) \to \mathbb{P}^1 \cong X(2)$ whose critical locus is disjoint from that of π. This can be done with an effective bound on the heights of all points in $\pi(f^{-1}\{0, 1, \infty\})$.

A dessin switch

We have seen that there exists a number field $F/\mathbb{Q}$ of a large degree but of bounded absolute ramification indices ($e = O(1)$), such that $d_F = \log\sqrt{D} + O(1)$ and E has everywhere good reduction over F. These properties are preserved as we adjoin the 10-torsion to F (because E/F has everywhere good reduction), hence we may assume the 10-torsion of E is rational over F.

A dessin switch

Choose one of the points of order 10 and consider the associated points $P \in Y(2)(F)$ and $Q \in Y(10)(F)$. Then replace P with $f(Q) \in Y(2)(F)$.

Applying $abc_{\Theta}^{\{2,\infty\}}$ on $f(Q) \in Y(2)(F)$ as discussed previously, we need to know the following to conclude:

Lemma: $h(f(Q)) - h^{\{2,\infty\}}(f(Q)) = O(\log D)$, with effective implied constant.

Applying the theorem of David and Hirata-Kohno

Lemma: $h(f(Q)) - h^{\{2,\infty\}}(f(Q)) = O(\log D)$, *with effective implied constant.*

Proof. It suffices to prove that all conjugates Q^σ satisfy

$$\log|j(f(Q^\sigma))|_v \ll \log D,$$

for $v \in \{2, \infty\}$. This follows from applying David and Hirata-Kohno's theorem as α runs through the finite set $j(\pi(f^{-1}\{0,1,\infty\})) \subset Y(1)(\bar{\mathbb{Q}}) = \bar{\mathbb{Q}}$.

Applying the theorem of David and Hirata-Kohno

Informally, the theorem of David and Hirata-Kohno shows that Q is not too near to the critical locus of f. Then $f(Q)$ is not too near to any of the cusps 0, 1 and ∞.

Applying the theorem of David and Hirata-Kohno

Informally, the theorem of David and Hirata-Kohno shows that Q is not too near to the critical locus of f. Then $f(Q)$ is not too near to any of the cusps 0, 1 and ∞.

Since the theory of logarithmic linear forms is effective, the implied constant of this estimate is effective.

Applying the theorem of David and Hirata-Kohno

Informally, the theorem of David and Hirata-Kohno shows that Q is not too near to the critical locus of f. Then $f(Q)$ is not too near to any of the cusps 0, 1 and ∞.

Since the theory of logarithmic linear forms is effective, the implied constant of this estimate is effective.

Note that a worse bound than $O(\log D)$ would not have sufficed. This uses the counterpart of Feldman's theorem, which had remained open for some time in the elliptic case.

IUT implies no Siegel zero at negative discriminants: conclusion

- By a dessin switch and an input from effective diophantine approximation theory, we have seen that $abc_{\Theta}^{\{2,\infty\}}$ implies $h(E/F) \ll \log D$ with effective implied constant.
- By $2h(E/F) = \sum_\rho \mathrm{Re}\,\frac{1}{1-\rho} + O(1)$, the last point implies $1 - \mathrm{Re}\,\rho \gg 1/\log D$ for all real zeros, with effective implied constant.

IUT implies no Siegel zero at negative discriminants: conclusion

- To close the gap between $abc_{\Theta}^{\{2,\infty\}}$ and [IUT-III, Cor. 3.12], it remains to insure the hypothesis on initial data in IUT-I, with $f(Q) \in Y(2)(F)$ replacing $P \in Y(2)(F)$, and with an $l \ll \log D$. This is done by following [AECGP, Theorem 3.8 (b)] and [IUT-IV, Cor. 2.2], replacing in *loc.cit.* assumptions of archimedeanly bounded moduli with the input $h_\infty(f(Q)) \ll \log D$ on the Archimedean part of the height, that we obtained from David and Hirata-Kohno's theorem.

Closing the gap from $abc_{\Theta}^{\{2,\infty\}}$ and IUT: some technical indication on insuring an admissible choice of l and $\mathbb{V}_{\mathrm{mod}}^{\mathrm{bad}}$

We are using the new elliptic curve E'/F of $j_{E'} = j(f(Q))$. There is a bounded degree extension F'/F over which E' has split semistable reduction. From David and Hirata-Kohno's theorem we have seen that the $\{2,\infty\}$-part of the stable Faltings height of E' satisfies $h_{\{2,\infty\}}(E'/F') \leq C \cdot \log D$, with an effective constant $C < \infty$.

Closing the gap from $abc_\Theta^{\{2,\infty\}}$ and IUT: some technical indication on insuring an admissible choice of l and $\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}$

For each prime l consider U_l the set of places $v \nmid 2, \infty$ of F' at which E' has a $\mathbb{G}_m$ reduction with l dividing the order of the q-parameter. If h_S denotes the S-part of the height, it is easily verified that $h(E'/F') \cdot \log h(E'/F') \gg \sum_l h_{U_l}(E'/F')$, where the log h is used as an upper bound on the maximum number of prime factors in the order of a q-parameter.

...some technical indication on insuring an admissible choice of l and $\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}$ (conclusion)

It follows from the last point that there are primes

$$l \asymp (\log h(E'/F'))^2 \tag{1}$$

meeting $h_{U_l}(E'/F') \leq h(E'/F')/4$. Assuming as we may that $h(E'/F') \geq 4C \cdot \log D$, we know also that $h_{\{2,\infty\}}(E'/F') \leq h(E'/F')/4$. Hence

$$h_{U_l \cup \{2,\infty\}}(E'/F') \leq h(E'/F')/2. \tag{2}$$

Closing the gap from $abc_{\Theta}^{\{2,\infty\}}$ and IUT: some technical indication on insuring an admissible choice of l and $\mathbb{V}_{\mathrm{mod}}^{\mathrm{bad}}$

Choose this l, and $\mathbb{V}_{\mathrm{mod}}^{\mathrm{bad}}$ the places $v \notin U_l$, $v \nmid 2, \infty$ of F at which E' has a $\mathbb{G}_m$ reduction. By (2), the argument of [AECGP, Lemma 3.5] applies as soon as $D \gg 1$, showing that E'/F' has no l-cyclic subgroup. Then the large Galois image in $\mathrm{Aut}(E[l])$ follows as in [AECGP], while (1) shows that [IUT-III, 3.12] applies at our choice $(E'/F'; l; \mathbb{V}_{\mathrm{mod}}^{\mathrm{bad}})$ to give $h(E'/F') \ll \log D$, just as with $abc_{\Theta}^{\{2,\infty\}}$.

May we hope to work Archimedeanly?

Restricting to the case of everywhere good reduction E/F, everything is Archimedean and classical. The Archimedean case was once taken as a prototype for the p-adic theory. Could we hope to work directly with the Archimedean places, without having to change to E'/F'?

May we hope to work Archimedeanly, and especially with CM?

The CM case as discussed before is particularly interesting; it has of course rich connections with algebraic and analytic number theory. Though of course it forbids the SL_2 hypothesis on the Galois image, we could still insure a transitive Galois action on $E[l]$. And if the CM features, instead of helping, are inherently antagonistic to the anabelian methods, we may easily find a polynomial dessin switch that removes the CM while retaining integral moduli.

A remark on the Archimedean analog of multiplicative subspaces

Since plane lattices could be more intuitive to visualize, let me mention the following regarding the Archimedean situation.

Assuming E/F has everywhere good reduction, then as noted before, the Faltings height $h(E/F)$ equals, up to $O(1)$, the average of $\pi y/3 - \log y$, where $y \geq 1$ ranges over the dilatations $y = \mathrm{Im}(\tau)$, $\tau = \omega_2/\omega_1$, of the complex period lattices of the conjugate elliptic curves.

A remark on the Archimedean analog of multiplicative subspaces

A degree-l isogeny $E \to E/C$ has the effect of stretching the dilatations by at most a factor of l, but usually, by the isogeny formula, the dilatations of E/C are much smaller. The places where the dilatation becomes $l \cdot y$ are the analogs of the primes where C is a multiplicative subspace. When $\mathrm{Gal}(K/F)$ is transitive on $E[l]$, we would start with any C and choose the section $\underline{\mathbb{V}} : \mathbb{V}_F \to \mathbb{V}_K$ to attain the highest possible dilatation $l \cdot y$ above each place of F. Since we aim for an inequality, we could as well regard $\underline{\mathbb{V}}$ as a completely arbitrary choice.

Extensions? Two inevitable points: 1.

Siegel zeros attached to CM fields would be similarly forbidden by an $\mathcal{A}_g$-version of IUT, i.e. a version for abelian varieties. IUT revolves around the crucial anabelian nature of the punctured elliptic curve, but similarly, the complement of any non-zero divisor in a simple abelian variety has strong hyperbolicity properties (e.g., Faltings proved it satisfies Siegel's finiteness property of integral points). It need not be a $K(\pi, 1)$, but what about replacing the étale fundamental group by étale homotopy type?

Extensions? Two inevitable points: 2.

And, finally, one is obliged of course to inquire about even characters, and real quadratic fields K. Instead of as CM points on $\mathbb{H}/\Gamma(1)$, the class group is realized as equal length closed geodesics on $\mathbb{H}/\Gamma(1)$, giving h continua of complex elliptic curves alongside the Kronecker-Hecke limit formula for $\frac{L'}{L}(1,\chi)\ldots$ and then?