Applications of IUT Theory to Diophantine Geometry and Equations over the rational numbers

Zhong-Peng Zhou

ITS, Westlake University

March 20, 2025

Introduction

In this talk, we explore the applications of Inter-universal Teichmüller (IUT) theory to two Diophantine problems:

- The effective abc inequalities over $\mathbb{Q}$
- The generalized Fermat equations

References

References:

- [IUTchI-IV] The *four main papers on IUT theory* by Mochizuki.
- [ExpEst] Shinichi Mochizuki, Ivan Fesenko, Yuichiro Hoshi, Arata Minamide, and Wojciech Porowski. *Explicit estimates in inter-universal Teichmüller theory*. Kodai Math. J., 45(2):175–236, 2022.
- [IUT-Q-I,II] Zhong-Peng Zhou. *The inter-universal Teichmüller theory and new Diophantine results over the rational numbers. I, II* (preprint). Available at: https://github.com/zhongpengzhou/Research-Papers

Effective abc inequalities, cf. [ExpEst]

In [IUTchIV], Mochizuki verified various *numerically non-effective* versions of the Vojta, ABC, and Szpiro Conjectures over number fields.

In [ExpEst], Mochizuki-Fesenko-Hoshi-Minamide-Porowski obtained various *numerically effective* versions of Mochizuki's results over $\mathbb{Q}$ and imaginary quadratic fields. For the case of $\mathbb{Q}$, they proved:

Theorem (Effective version of a conjecture of Szpiro)

Let a, b, c be non-zero coprime integers such that $a + b + c = 0$; ϵ a positive real number ≤ 1. Then we have

$$|abc| \leq 2^4 \cdot \max\{\exp(1.7 \cdot 10^{30}) \cdot \epsilon^{-166/81}, \mathrm{rad}(abc)^{3+3\epsilon}\}.$$

Effective abc inequalities (2)

Corollary 1

Fermat's Last Theorem (FLT) holds for prime exponents $> 1.615 \cdot 10^{14}$.

This work, combined with the results of Vandiver, Coppersmith, and Mihăilescu-Rassias, yields an **unconditional new alternative proof** of Fermat's Last Theorem (FLT).

Corollary 2

When $r, s, t > 2.453 \cdot 10^{30}$, the generalized Fermat equation $x^r + y^s = z^t$ has no positive coprime integer solution.

Question: Can we prove stronger abc inequalities, and prove stronger results towards the generalized Fermat equations?

Applications of IUT to effective abc ineqs., cf. [IUT-Q-I]

Flowchart:

Construction of initial Θ-data →	Estimation of log-volumes →	Diophantine results i.e. abc inequalities
Focusing on elliptic curves over $\mathbb{Q}$	Sightly modified estimation	Deducing from "partial" inequalities

Construction of initial Θ-data, cf. [IUT-Q-I], §2

As defined in [IUTchIV] and [ExpEst], a μ_6-initial Θ-data $(\overline{F}/F, X_F, \ell, \underline{C}_K, \underline{\mathbb{V}}, \mathbb{V}_{\mathrm{mod}}^{\mathrm{bad}}, \underline{\epsilon})$ consists of the following objects:

- An *elliptic curve* E_F over a *number field* F; denote $X_F = E_F \setminus \{O\}$, $F_{\mathrm{mod}} = \mathbb{Q}(j(E_F))$, assume F/F_{mod} is Galois and $F(\sqrt{-1}, E_F[6]) = F$.
- A *prime number* $\ell \geq 5$, s.t. $\ell \nmid [F : F_{\mathrm{mod}}]$; Denote $K = F(E_F[\ell])$, and assume that the image of the mod ℓ Galois repr. of E_F

$$\rho_{E_F,\ell} : G_F \twoheadrightarrow \mathrm{Gal}(F(E_{\overline{F}}[l])/F) \to \mathrm{Aut}(E_{\overline{F}}[l]) \cong \mathrm{GL}(2, \mathbb{F}_\ell)$$

  contains the subgroup $\mathrm{SL}(2, \mathbb{F}_\ell) \subseteq \mathrm{GL}(2, \mathbb{F}_\ell)$.
- A non-empty collection of "bad" *valuations* $\mathbb{V}_{\mathrm{mod}}^{\mathrm{bad}} \subseteq \mathbb{V}_{\mathrm{mod}}$.
- A *curve* $\underline{C}_K$ with K-core $C_K = X_K/\{\pm 1\}$, where $X_K = X_F \times_F K$.
- A *section* $\eta : \mathbb{V}_{\mathrm{mod}} \xrightarrow{\sim} \underline{\mathbb{V}} \subseteq \mathbb{V}(K)$ of $\mathbb{V}(K) \twoheadrightarrow \mathbb{V}_{\mathrm{mod}}$.

There are some more definitions and assumptions.

Construction of initial Θ-data (2)

Notations. For a μ_6-initial Θ-data

$$\mathfrak{D} = (\overline{F}/F, X_F, \ell, \underline{C}_K, \underline{\mathbb{V}}, \mathbb{V}_{\mathrm{mod}}^{\mathrm{bad}}, \underline{\epsilon})$$

with $F_{\mathrm{mod}} = \mathbb{Q}$, let N be the denominator of the j-invariant $j(E_F) \in \mathbb{Q}$, and let N' be the maximal divisor of N whose prime divisors corresponds to places in $\mathbb{V}_{\mathrm{mod}}^{\mathrm{bad}}$, i.e.

$$N' := \prod_{p\colon\, v_p \in \mathbb{V}_{\mathrm{mod}}^{\mathrm{bad}}} p^{v_p(N)}.$$

Then we have $\log(N') = \log(\mathfrak{q})$ in the notation of [IUTchIV], Theorem 1.10. We shall say $\mathfrak{D}$ is **of type** $(\boldsymbol{\ell}, \boldsymbol{N}, \boldsymbol{N'})$.

Construction of initial Θ-data (3)

Proposition

Let E be an elliptic curve defined over $\mathbb{Q}$; N be the denominator of $j(E)$; F be a number field Galois over $\mathbb{Q}$; $\ell \geq 11$ be a prime number such that $\ell \nmid [F : \mathbb{Q}]$; $E_F := E \times_{\mathbb{Q}} F$, $X_F = E_F \setminus \{O\}$. Suppose that:

(1) $\sqrt{-1} \in F$, $F(E[6]) = F$, E_F is semi-stable, and $F \subseteq \mathbb{Q}(E[n])$ for some positive integer $\ell \nmid n$.

(2) $j(E) \notin \{0, 2^6 \cdot 3^3, 2^2 \cdot 73^3 \cdot 3^{-4}, 2^{14} \cdot 31^3 \cdot 5^{-3}\}$.

(3) We have $\ell \neq 13$ and N is not a power of 2; or E is semi-stable.

(4) We have $N'_\ell \neq 1$, where $N'_\ell := \prod_{p : p \neq \ell, \ell \nmid v_p(N)} p^{v_p(N)}$.

Then there exists a μ_6-initial Θ-data $\mathfrak{D} = (\overline{F}/F, X_F, \ell, \underline{C}_K, \underline{\mathbb{V}}, \mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}, \underline{\epsilon})$, which is of type (ℓ, N, N'_ℓ).

Construction of initial Θ-data (4)

Remark. In the previous proposition:

- (1) $\Rightarrow$ the image of the mod ℓ repr. $\rho_{E_F,\ell}$ of E_F equals that of E.
- (3), (4) $\Rightarrow$ the mod ℓ repr. $\rho_{E,\ell}$ of E is surjective, cf. Mazur, "Rational isogenies of prime degree (with an appendix by D. Goldfeld)",
- (2) $\Rightarrow$ C_K is the K-core of $\underline{C}_K$ and X_K, cf. [ExpEst], Proposition 2.1, also cf. Sijsling, "Canonical models of arithmetic $(1; e)$-curves".
- (4) $\Rightarrow$ $\mathbb{V}^{\text{bad}}_{\text{mod}} \neq \emptyset$.
- If the image of $\rho_{E,\ell}$ contains $\mathrm{SL}(2, \mathbb{F}_\ell)$, then $\exists$ suitable $\underline{C}_K, \underline{\mathbb{V}}, \underline{\epsilon}$, which constitute a μ_6-initial Θ-data $(\overline{F}/F, X_F, \ell, \underline{C}_K, \underline{\mathbb{V}}, \mathbb{V}^{\text{bad}}_{\text{mod}}, \underline{\epsilon})$.
- $v_p \notin \mathbb{V}_{\text{mod}}$ if and only if $p = \ell$ or $\ell \mid v_p(N)$, hence "$N' = N'_\ell$".

The μ_6-initial Θ-data associated to "$a+b=c$"

Let (a, b, c) be a triple of non-zero coprime integers such that $a+b=c$.
Let $\ell \geq 11$, $\ell \neq 13$ be a prime number, cf. (3).
Let $N = a^2b^2c^2 / \gcd(2^8, a^2b^2c^2)$, $N'_\ell = \prod_{p: p\neq\ell, \ell\nmid v_p(N)} p^{v_p(N)}$.
Suppose that:

- $(|a|, |b|, |c|)$ is not a permutation of $(1,1,2)$, $(1,8,9)$, cf. (2).
- $N'_\ell \neq 1$, cf. (4).

Let E be the Frey-Hellegouarch curve associated to (a, b, c), which is defined over $\mathbb{Q}$ by the equation $y^2 = x(x-a)(x+b)$.

The μ_6-initial Θ-data associated to "$a+b=c$" (2)

Write $F = \mathbb{Q}(\sqrt{-1}, E[3])$, then:

- N is the denominator of $j(E) = 256(a^2+ab+b^2)^3/a^2b^2c^2$.
- F is Galois over $\mathbb{Q}$, $\sqrt{-1} \in F$, $F(E[6]) = F$, E_F is semi-stable, and $F \subseteq \mathbb{Q}(E[12])$, cf. (1).

Thus, based on the previous proposition $\Rightarrow$

There exists a μ_6-initial Θ-data

$$\mathfrak{D}(E, F, \ell, \mu_6) = (\overline{F}/F, X_F, \ell, \underline{C}_K, \underline{\mathbb{V}}, \mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}, \underline{\epsilon}),$$

which is **of type** $(\ell, \boldsymbol{N}, \boldsymbol{N}'_\ell)$.

Estimation of log-volumes, cf. [IUT-Q-I], §1

In this part, we shall make use of [IUTchIII], Corollary 3.12 and its μ_6-version in [ExpEst], which play key roles in the application in [IUT-Q-I] and [IUT-Q-II]. The proofs of them relies on strong anabelian geometry results primarily established by Mochizuki.

Theorem (cf. [IUTchIV], [ExpEst])

$$-|\log(\underline{\underline{\mathfrak{q}}})| \leq -|\log(\underline{\underline{\Theta}})|$$

By estimating $-|\log(\underline{\underline{\Theta}})|$, we can obtain upper bounds for $-|\log(\underline{\underline{\mathfrak{q}}})|$.

Estimation of log-volumes (2)

Notations.

Let $\mathfrak{D} = (\overline{F}/F, X_F, \ell, \underline{C}_K, \underline{\mathbb{V}}, \mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}, \underline{\epsilon})$ be a μ_6-initial Θ-data, such that $F_{\mathrm{mod}} = \mathbb{Q}$. Let N be the denominator of $j(E_F)$.
Suppose that $\mathfrak{D}$ is of type (ℓ, N, N').

For each $v_p \in \mathbb{V}^{\mathrm{non}}_{\mathbb{Q}}$, let $\underline{v}_p := \eta(v_p) \in \underline{\mathbb{V}} \subseteq \mathbb{V}(K)^{\mathrm{non}}$. Write e_p for the **ramification index** of $K_{\underline{v}_p}$ over $\mathbb{Q}_p$; write $d_p \in \frac{1}{e_p} \cdot \mathbb{Z}$ for the **different index** of $K_{\underline{v}_p}$, i.e. the p-adic valuation of any generator of the different ideal of the ring of integers of $K_{\underline{v}_p}$ over $\mathbb{Z}_p$.

We have $d_p = 0$ when $e_p = 1$; $d_p = 1 - \frac{1}{e_p}$ when $p \nmid e_p$; $d_p \leq 1 + v_p(e_p)$ when $p \mid e_p$ [cf. [IUTvhIV], Proposition 1.3].

Estimation of log-volumes (3)

Proposition

$$\frac{1}{6}\log(N') \leq \frac{\ell^2+5\ell}{\ell^2+\ell-12}\cdot\Big(\log(\pi)+\sum_{e_p\geq p-1}\big(\frac{1}{p-1}+1-\frac{p-1}{e_p}\big)\cdot\log(p)$$
$$+\sum_{p\geq 2}d_p\cdot\log(p)+\sum_{e_p>p(p-1)}\log\big(\frac{e_p}{p-1}\big)\Big).$$

Remark. In [IUTchIV] and [ExpEst], the inequality $e_p \leq [K:\mathbb{Q}]$ is used to get an upper bound of the RHS of the inequality in the above proposition. However, for special classes of elliptic curves, one may prove smaller upper bounds for e_p.

Partial abc inequalities, cf. [IUT-Q-I], §2

Example for the μ_6-initial Θ-data associated to "$a+b=c$".

- For $p \neq 2, 3, \ell$, if $p \mid abc$, then $e_p \mid 3\ell$, $d_p = 1 - \frac{1}{e_p} \leq 1 - \frac{1}{3\ell}$; if $p \nmid abc$, then $e_p = 1$, $d_p = 0$.
- For $p \in \{3, \ell\}$, if $p \mid abc$, then $e_p \in (p-1) \cdot \{1, 3, \ell, 3\ell\}$, $d_p \leq 2$; if $p \nmid abc$, then $e_p \in \{p-1, p(p-1), p^2-1\}$, $d_p \leq 2$.
- For $p = 2$, if $v_2(abc) \geq 5$, then $e_2 \in \{2, 6, 2\ell, 6\ell\}$, $d_2 \leq 2$; if $1 \leq v_2(abc) \leq 4$, then $2 \mid e_2$, $e_2 \mid 48$ and $d_2 \leq 1 + v_2(e_2) \leq 5$.

Partial abc inequalities (2)

Proposition (Partial abc inequality)

Let (a, b, c) be a triple of non-zero coprime integers such that $a + b = c$, let $\ell \geq 11$ be a prime number s.t. $\ell \neq 13$, let $N = |abc| / \gcd(16, abc)$.

Then there exists a real number $\mathrm{Vol}(\ell) \geq 0$ [which only depends on ℓ], s.t.

$$\log\Big(\prod_{p : p \neq \ell, \ell \nmid v_p(N)} p^{v_p(N)}\Big) \leq \Big(3 + \frac{11\ell + 31}{\ell^2 + \ell - 12}\Big) \cdot \log \mathrm{rad}(N) + 3\,\mathrm{Vol}(\ell).$$

Here we have $\mathrm{Vol}(\ell) < \frac{3}{2} \cdot \ell + 0.06 \cdot \frac{\ell}{\log(\ell)}$ for $\ell \geq 2 \cdot 10^5$.

Effective abc inequaties, cf. [IUT-Q-I], §3

Rather than $\log(N)$, the left hand of the partial abc inequality equals

$$\log\Big(\prod_{p:\,p\neq\ell,\,\ell\nmid v_p(N)} p^{v_p(N)}\Big) = \log(N) - \underbrace{\sum_{p:\ p=\ell \text{ or } \ell | v_p(N)} v_p(N)\cdot\log(p)}_{\text{the error term at } \ell},$$

which depends on ℓ. This is why it is called "partial abc inequality".

Question: How to deduce effective abc inequaties from partial ones?

In [IUT-Q-I], we control the error term by averaging the partial abc inequalities over a suitable finite set S of ℓ.

Effective abc inequaties (2)

Theorem

Let (a, b, c) be a triple of non-zero coprime integers such that $a + b = c$. Suppose that $\log(|abc|) \geq 700$, then we have

$$\log(|abc|) \leq 3 \log \mathrm{rad}(abc) + 8\sqrt{\log(|abc|) \cdot \log\log(|abc|)}.$$

Corollary

Let (a, b, c) be a triple of non-zero coprime integers such that $a + b = c$; let ϵ be a positive real number $\leq \frac{1}{10}$. Then we have

$$|abc| \leq \max\{\exp\left(400 \cdot \epsilon^{-2} \cdot \log(\epsilon^{-1})\right), \mathrm{rad}(abc)^{3+3\epsilon}\}.$$

Generalized Fermat equations

Let $r, s, t \geq 2$ be positive integers. The equation

$$x^r + y^s = z^t, \text{ with } x, y, z \in \mathbb{Z}$$

is known as the **generalized Fermat equation** (GFE) with **signature** (r, s, t).

A solution (x, y, z) to the generalized Fermat equation is called **non-trivial** if $xyz \neq 0$; **positive** if $x, y, z \in \mathbb{Z}_{\geq 1}$; and **primitive** if $\gcd(x, y, z) = 1$.

When $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} \leq 1$, only the **Catalan solution** $1^n + 2^3 = 3^2$ and the following **nine non-Catalan** solutions are currently known:

$$\begin{aligned}
&2^5 + 7^2 = 3^4, && 17^7 + 76271^3 = 21063928^2, && 1414^3 + 2213459^2 = 65^7,\\
&7^3 + 13^2 = 2^9, && 9262^3 + 15312283^2 = 113^7, && 43^8 + 96222^3 = 30042907^2,\\
&2^7 + 17^3 = 71^2, && 3^5 + 11^4 = 122^2, && 33^8 + 1549034^2 = 15613^3.
\end{aligned}$$

Generalized Fermat equations (2)

In [IUT-Q-I, II], the following previously established results are used to excluded proven signatures.
The generalized Fermat equation $x^r + y^s = z^t$ admits no non-trivial primitive solutions, except for the solutions potentially associated with the Catalan solutions and the nine non-Catalan solutions, when (r, s, t) is a **permutation** of:

- $(n, n, n), n \geq 3$; $(2, n, n), n \geq 4$; $(3, n, n), n \geq 3$;
- $(2, 3, n)$, $n \in \{6, 7, 8, 9, 10, 15\}$; $(2, 4, n), n \geq 4$; $(2, 6, n), n \geq 3$;
- $(3, 3, n), 3 \leq n \leq 10^9$; $(3, 4, 5)$, $(5, 5, 7)$, $(5, 7, 7)$;
- $(5, 5, q)$, prime $q \geq 11 > 3\sqrt{5 \log_2(5)}$.

Catalan's conjecture proven by Mihăilescu is also used in these two papers.

Preliminary applications of IUT to GFE, cf. [IUT-Q-I], §4

Flowchart:

$$\boxed{\text{Construction of initial } \Theta\text{-data}} \longrightarrow \boxed{\text{Estimation of log-volumes}} \longrightarrow \boxed{\text{The generalized Fermat equations}}$$

Theorem

For positive primitive solutions (x, y, z) to the generalized Fermat equation $x^r + y^s = z^t$ $(r, s, t \geq 3)$, define $h = \log(x^r y^s z^t)$. Then we prove explicit upper bounds:

$$h \leq 573 \ \ (r, s, t \geq 8); \ \ h \leq 907 \ \ (r, s, t \geq 5); \ h \leq 2283 \ \ (r, s, t \geq 4);$$
$$h \leq 14750 \ \ (\min\{r, s\} \geq 4 \text{ or } t \geq 4); \ h \leq 24626 \ \ (r, s, t \geq 3).$$

Preliminary applications of IUT to GFE (2)

Some corollaries:

(1) FLT holds for prime exponents ≥ 11.

(2) When r, s, t is a permutation of $(3, 3, n)$ $(n \geq 3)$, the GFE $x^r + y^s = z^t$ admits no non-trivial primitive solution.

(3) When $r, s, t \geq 20$, the GFE $x^r + y^s = z^t$ admits no non-trivial primitive solution.

Question. How to prove for smaller signatures/exponents $(\boldsymbol{r}, \boldsymbol{s}, \boldsymbol{t})$?

Refined applications of IUT to GFE, cf. [IUT-Q-II]

Refined flowchart:

$$\begin{tikzcd}
\boxed{\begin{matrix}\text{Construction of} \\ \text{initial } \Theta\text{-data}\end{matrix}} \arrow[r] & \boxed{\begin{matrix}\text{Estimation of} \\ \text{log-volumes}\end{matrix}} \arrow[r] & \boxed{\begin{matrix}\text{The generalized} \\ \text{Fermat equation}\end{matrix}} \\
\boxed{\begin{matrix}\text{2-torsion version} \\ \text{of IUT theory}\end{matrix}} \arrow[u, dashed] & \boxed{\begin{matrix}\text{Partial inequalities} \\ \text{for given solutions}\end{matrix}} \arrow[u, dashed] & \boxed{\begin{matrix}\text{The ``structure''} \\ \text{of given solutions}\end{matrix}} \arrow[u, dashed]
\end{tikzcd}$$

2-torsion version of IUT theory, cf. [IUT-Q-II], §1.1

Definition. We shall refer to **2-torsion initial Θ-data** as any collection of data $(\overline{F}/F, X_F, \ell, \underline{C}_K, \underline{\mathbb{V}}, \mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}, \underline{\epsilon})$ satisfying the following conditions:

- The conditions in [IUTchI], Definition 3.1, (a), (c), (d), (e), (f).
- The "2-torsion version" of [IUTchI], Definition 3.1, (b), i.e., the condition obtained by replacing, in [IUTchI], Definition 3.1, (b), "$2 \cdot 3$-torsion points of E_F are rational over F", by "2-torsion points of E_F are rational over F, and E_F has a model over F_{mod}".

Comparison:

IUT version	About $\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}$	About F
the original version	not dividing 2	$F(E_F[6], \sqrt{-1}) = F$
the μ_6-version	/	$F(E_F[6], \sqrt{-1}) = F$
the 2-torsion version	not dividing 2	$F(E_F[2], \sqrt{-1}) = F$ and E_F has a model E over F_{mod}

2-torsion version of IUT theory (2)

It is worth noting that the results of [IUTchI-IV] still hold for its 2-torsion version, i.e. by replacing initial Θ-data with 2-torsion initial Θ-data. In these papers, the condition "3-torsion points of E_F are rational over F", i.e. "$F(E[3]) = F$" is only used in [IUTchI], Remark 3.1.5, [IUTchIV], Theorem 1.10 and [IUTchIV], Corollary 2.2 via [IUTchIV], Proposition 1.8, (iv), (v).

As a consequence of "$F(E[3]) = F$", it is stated that K is Galois over F_{mod} at the beginning of [IUTchI], Remark 3.1.5. This still holds for its 2-torsion version. Since E_F has a model E defined over F_{mod}, we can put $L = F_{\text{mod}}(E[\ell])$, then L/F_{mod} is Galois. Since F/F_{mod} is Galois by the definition of [2-torsion] initial Θ-data, we can see that $K = F(E_F[\ell]) = F \cdot L$ is Galois over F_{mod}.

2-torsion version of IUT theory (3)

The condition "$F(E[3]) = F$" is also used to show that E_F has a model over F_{mod} in [IUTchIV], Theorem 1.10 and [IUTchIV], Corollary 2.2, after an initial Θ-data is constructed. This is one of the conditions in the definition of 2-torsion initial Θ-data.

Hence the results of [IUTchI-IV] (especially [IUTchIII], Corollary 3.12) **still hold** for their 2-torsion versions. The 2-torsion versions of "proposition for the construction of 2-torsion initial Θ-data with $F_{\text{mod}} = \mathbb{Q}$" and "partial inequalities" [which is based on the 2-torsion version of [IUTchIII], Corollary 3.12] can similarly be proven.

Partial inequalities for solutions, cf. [IUT-Q-II], §2

Let $\boldsymbol{r}, \boldsymbol{s}, \boldsymbol{t} \geq \mathbf{4}$ be positive integers, (x, y, z) be a triple of positive coprime integers such that $\delta_r x^r + \delta_s y^s = z^t$, where $\delta_r, \delta_s \in \{\pm 1\}$. Let $\ell \geq 11$ be a prime number.

Let (a, b, c) be a permutation of $(\delta_r x^r, \delta_s y^s, -z^t)$, such that $4 \mid (a+1)$ and $16 \mid b$. Then $a + b + c = 0$, $\gcd(a, b, c) = 1$.

Let E be the elliptic curve defined over $\mathbb{Q}$ by the equation

$$Y^2 + XY = X^3 + \frac{b-a-1}{4} \cdot X^2 - \frac{ab}{16} \cdot X.$$

Then E is a semi-stable elliptic curve.

Partial inequalities for solutions (2)

Let $N = 2^{-8}x^{2r}y^{2s}z^{2t}$, then N is the denominator of $j(E)$.
Let $F = \mathbb{Q}(\sqrt{-1})$, $E_F = E \times_{\mathbb{Q}} F$.

Then there exists a 2-torsion initial Θ-data $\mathfrak{D} = \mathfrak{D}(E, F, \ell, 2\text{-tor})$ which is of type $(\ell, N, N'_{2\ell})$, where $N'_{2\ell} = \prod_{p\colon p\nmid 2\ell,\, \ell\nmid v_p(N)} p^{v_p(N)}$.

In this case, we have $e_p = 1, d_p = 0$ or $e_p = \ell, d_p = 1 - \frac{1}{\ell}$ for $p \neq 2, \ell$.
By the estimation of log-volumes, for some real number $\mathrm{Vol}(\ell) \geq 0$, we have the following partial inequality for solutions:

Proposition (Partial inequality for given solutions)

$$\frac{1}{3}\log\Big(\prod_{p\colon p\nmid 2\ell,\, \ell\nmid v_p(x^r y^s z^t)} p^{v_p(x^r y^s z^t)}\Big) \leq \frac{(\ell+5)(\ell-1)}{\ell^2+\ell-12} \cdot \sum_{p\colon \ell\nmid v_p(x^r y^s z^t)} \log(p) + \mathrm{Vol}(\ell),$$

Partial inequalities for solutions (3)

Let $a_1(\ell) = 3 \cdot \frac{(\ell+5)(\ell-1)}{\ell^2+\ell-12}$, $a_2(\ell) = 3 \cdot \mathrm{Vol}(\ell) + a_1(\ell) \cdot \log(2\ell)$.
Then $3 < a_1(\ell) \leq 4$, $a_2(11) \leq 71$, $a_2(13) \leq 74$, etc., and we have:

Corollary

$$\sum_{p:\ p \nmid 2\ell,\ \ell \nmid v_p(x^r y^s z^t)} (v_p(x^r y^s z^t) - 4) \cdot \log(p) \leq a_2(\ell).$$

Remark. (1) To reduce "the number of possible solutions" to GFE in the subsequent steps, the smaller the values of $\mathrm{Vol}(\ell)$ and $a_2(\ell)$, the better.
(2) These values depend on the values of various e_p, which is why we focus on the Frey-Hellegouarch curves and introduce a 2-torsion version of IUT theory.
(3) Since $r, s, t \geq 4$, we can replace the LHS by its partial sum.

Structure of solutions, cf. [IUT-Q-II], §2

Suppose that $\ell \nmid r$ and consider the unique decomposition

$$x = x_1 \cdot 2^{r_2} \cdot \ell^{r_\ell} \cdot x_\ell^\ell, \quad \text{where } x_\ell = \prod_{p:\, p \nmid 2\ell,\, \ell | v_p(x)} p^{v_p(x)} \text{ and } \gcd(2\ell, x_1) = 1.$$

Then by the corollary, we have:

$$\log(x_1) - 4 \log \operatorname{rad}(x_1) \leq a_2(\ell).$$

Using the above inequality for different ℓ, we can prove the following:

Proposition

(1) We have $r \leq 313$, $r_2 \leq \frac{306}{r}$, $r_\ell \leq \frac{37}{r}$.

(2) We have $x_\ell \in \{1, 3, 5\}$ if $(r, \ell) = (4, 11)$; $x_\ell \in \{1, 3\}$ if $(r, \ell) = (4, 13), (4, 17), (5, 11), (5, 13), (6, 11)$; and $x_\ell = 1$ otherwise.

Structure of solutions (2)

Suppose that $\ell \nmid rs$ and consider the similar unique decompositions

$$x = x_1 \cdot 2^{r_2} \cdot \ell^{r_\ell} \cdot x_\ell^\ell, \quad y = y_1 \cdot 2^{s_2} \cdot \ell^{s_\ell} \cdot y_\ell^\ell,$$

Then we have similar upper bounds for s, s_2, s_ℓ, y_ℓ by the proposition.

Meanwhile, by the corollary, we have

$$(r-4)\log(x_1) + (s-4)\log(y_1) \leq a_2(\ell).$$

Hence for each fixed signature (r, s, t), there are only finitely many possible (x_1, y_1) and finitely many possible $(r_2, s_2, r_\ell, s_\ell, x_\ell, y_\ell)$, hence only **finitely many possible** (x, y).

By checking whether $|\pm x^r \pm y^s|$ is a t-th power for all possible (x, y), we can find all positive coprime integers (x, y, z) satisfying $\delta_r x^r + \delta_s y^s = z^t$, where $\delta_r, \delta_s \in \{\pm 1\}$.

Conclusions, cf. [IUT-Q-II]

After implementing the search algorithm, we have computed all signatures where $r \leq s \leq t$ and $r + s \geq 12$, excluding those already solved:

Proposition

For any integers $r, s, t \geq 4$, such that (r, s, t) is not a permutation of $(4, 5, n), (4, 7, n), (5, 6, n)$ with $7 \leq n \leq 301$, the generalized Fermat equation

$$x^r + y^s = z^t$$

admits no non-trivial primitive solution.

Remark. By rough estimation, the search for signatures $(4, 7, n)$, $(5, 6, n)$ is computable [at least for large n], but it needs at least hundreds of hours of wall clock time in total.

Conclusions (2)

In [IUT-Q-II], the signatures (r, s, t) with $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$ are divided into four classes. Each class can be researched by using different classes of [modified] Frey-Hellegouarch curves:

Signatures Up To Permutations	Curves & Conditions
$r, s, t \geq 4$	$Y^2 + XY = X^3 + \frac{b-a-1}{4} \cdot X^2 - \frac{ab}{16} \cdot X$, $a + b = c$ coprime, $4 \mid (a+1)$ and $16 \mid b$
$(2, 3, t),\ t \geq 7$	$Y^2 = X^3 + 3bX + 2a,\ a^2 + b^3 = c$ coprime
$(3, r, s),\ r \geq 3,\ s \geq 4$	$Y^2 + 3cXY + aY = X^3,\ a + b = c^3$ coprime
$(2, r, s),\ r \geq 4,\ s \geq 5$	$Y^2 = X^3 + 2cX^2 + aX,\ a + b = c^2$ coprime

Conclusions (3)

Theorem

Let $r, s, t \geq 2$ be positive integers such that $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} \leq 1$. Then the generalized Fermat equation $x^r + y^s = z^t$ admits no non-trivial primitive solution, exceplt for the solutions related to the Catalan solutions $1^n + 2^3 = 3^2$ and nine non-Catalan solutions, when (r, s, t) is not a permutation of the following signatures:

- $(4, 5, n)$, $(4, 7, n)$, $(5, 6, n)$, with $7 \leq n \leq 303$.
- $(2, 3, n)$, $(3, 4, n)$, $(3, 8, n)$, $(3, 10, n)$, with $11 \leq n \leq 109$ or $n \in \{113, 121\}$.
- $(3, 5, n)$, with $7 \leq n \leq 3677$; $(3, 7, n)$, $(3, 11, n)$, with $11 \leq n \leq 667$.
- $(3, m, n)$, with $13 \leq m \leq 17$, $m < n \leq 29$; $(2, m, n)$, with $m \geq 5$, $n \geq 7$.

Conclusions (4)

Remark. (1) We have worked on the first three classes of signatures. For permutations of $(2, m, n)$, $m \geq 5$, $n \geq 7$, the related work will be undertaken in future studies.

(2) We can continue to exclude the multiples of some solved signatures, e.g., $(4, 5, 2n)$, $(4, 5, 3n)$, $(4, 5, 5n)$ with $n \geq 1$.

Corollary

To solve the generalized Fermat equation $x^r + y^s = z^t$ with exponents $r, s, t \geq 4$, we are left with 244 signatures (r, s, t) up to permutation; to solve the Beal conjecture, we are left with 2446 signatures (r, s, t) up to permutation.