The inter-universal Teichmüller theory and new Diophantine results over rational numbers. II

Zhong-Peng Zhou

Abstract

[This is an older version of the paper, which will be updated soon.]

In the present paper, we continue our research on the generalized Fermat equation $x^r + y^s = z^t$ with signature (r, s, t), where $r, s, t \geq 2$ are positive integers such that $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$. All known positive primitive solutions for the generalized Fermat equation when $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1$ are related to the Catalan solutions $1^n + 2^3 = 3^2$ and nine non-Catalan solutions.

By applying inter-universal Teichmüller theory and its slight modification in the case of elliptic curves over rational numbers, we deduce that the generalized Fermat equation $x^r + y^s = z^t$ has no non-trivial primitive solution except for those related to the Catalan solutions and nine non-Catalan solutions mentioned above, 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 $m \geq 5$, $n \geq 7$.

As a 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.

Introduction

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

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

is known as the generalized Fermat equation with signature (r, s, t). A solution (x, y, z) to $(\star)$ is called non-trivial if $xyz \neq 0$, positive if $x, y, z \in \mathbb{Z}_{\geq 1}$, and primitive if $\gcd(x, y, z) = 1$.

Finding all the positive primitive solutions to $(\star)$ is a long-standing problem in number theory. The Pythagorean triples, which are the positive solutions to $(\star)$ with signature $(2, 2, 2)$, have been known since ancient times. Fermat's Last Theorem, proven by Wiles in 1994 [36], states that $(\star)$ has no positive primitive solution with signature (n, n, n) for $n \geq 3$. Catalan's conjecture, proven by Mihăilescu in 2002 [23], states that if $x = 1$ in $(\star)$, then the only positive integer solution to $1 + y^s = z^t$ (with $s, t \geq 2$) is $(y, z, s, t) = (2, 3, 3, 2)$.

The behavior of positive primitive solutions to $(\star)$ is fundamentally determined by the size of the quantity

$$\chi(r, s, t) = \frac{1}{r} + \frac{1}{s} + \frac{1}{t} - 1.$$

Here, χ is the Euler characteristic of a certain stack associated with $(\star)$.

For the spherical case where $\chi > 0$, (r, s, t) is a permutation of $(2, 2, t)$, $t \geq 2$, or $(2, 3, t)$, $3 \leq t \leq 5$. In this case, parametrizations for positive primitive solutions for these signatures can be found in Beukers [7], Edwards [20], and Cohen [15], Section 14.

For the Euclidean case where $\chi = 0$, (r, s, t) is a permutation of $(2, 3, 6)$, $(2, 4, 4)$, or $(3, 3, 3)$. In this case, non-trivial primitive solutions for these signatures come from the Catalan solution $1^6 + 2^3 = 3^2$, cf. [4], Proposition 6 for a proof.

For the hyperbolic case where $\chi < 0$, the number of primitive solutions for each fixed signature (r, s, t) is finite, cf. Darmon-Granville [18]. For this case, only the Catalan solution $1^n + 2^3 = 3^2$ and the following nine non-Catalan solutions are currently known:

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

Since all known solutions have $\min\{r, s, t\} \leq 2$, Beal conjectured in 1993 [22] that the generalized Fermat equation $(\star)$ has no positive primitive solution when $r, s, t \geq 3$. This conjecture is known as the Beal conjecture, also known as the Mauldin conjecture and the Tijdeman-Zagier conjecture.

For many signatures (r, s, t) with $\chi \leq 0$, the generalized Fermat equation $x^r + y^s = z^t$ has been proved to have no other non-trivial primitive solution, except for the possible solutions related to the Catalan solution and the nine non-Catalan solutions listed above. Some of these signatures needed in this paper are listed below, which is used to avoid repeated computation for some proven cases during the search for possible solutions:

- $(n, n, n), n \geq 3$, cf. Wiles [36], Taylor-Wiles [35], Mochizuki-Fesenko-Hoshi-Minamide-Porowski [28].
- $(n, n, 2), n \geq 4$; $(n, n, 3), n \geq 3$, cf. Darmon-Merel [19], Poonen [29].
- $(2, 3, n), n \in \{7, 8, 9, 10, 15\}$, cf. Poonen-Schaefer-Stoll [30], Bruin [10, 12], Brown [9], Siksek-Stoll [33].
- $(2, 4, n), n \geq 4$, cf. Ellenberg [21], Bennett-Ellenberg-Ng [5]; $(2, n, 4), n \geq 4$, Corollary of Bennett-Skinner [6], Bruin [11].
- $(2, 6, n), n \geq 3$, cf. Bennett-Chen [3]; $(2, n, 6), n \geq 3$, cf. Bennett-Chen-Dahmen-Yazdani [4].
- $(3, 3, n), n \geq 3$, cf. Chen-Siksek [14], Zhou [38].
- $(3, 4, 5)$, $(5, 5, 7)$, $(5, 7, 7)$, cf. Siksek-Stoll [32], Dahmen-Siksek [17].
- $(5, 5, q)$, primes $q \geq 11 > 3\sqrt{5 \log_2(5)}$, cf. Bartolomé-Mihăilescu [2].

In 2022, Mochizuki, Fesenko, Hoshi, Minamide, and Porowski [28] established a μ_6-version of Mochizuki's inter-universal Teichmüller theory (IUT theory), cf. [24, 25, 26, 27], which managed to "treat" bad places that divide the prime 2. They then verified the numerically effective versions of the Vojta, ABC, and Szpiro Conjectures over the rational numbers and imaginary quadratic number fields. As a result, they verified that Fermat's Last Theorem (FLT) holds for prime exponents $> 1.615 \cdot 10^{14}$ — which is sufficient, combined with the results of Vandiver, Coppersmith, and Mihăilescu-Rassias, to yield an unconditional new alternative proof of Fermat's Last Theorem.

For the first time proving effective abc inequalities and containing a new proof of FLT, the paper [28] sheds light on solving generalized Fermat equations. In the previous paper [38], by making slight modifications to the estimation in [27] and [28], we reduced the coefficient of the effective abc inequality presented in [28], and performed a preliminary study on the generalized Fermat equation $x^r + y^s = z^t$ with exponents $r, s, t \geq 3$.

In the present paper, in order to further study more situations, the signatures with $\chi < 0$ are divided into four cases. For each of these cases, we can use different classes of [modified] Frey-Hellegouarch curves in IUT theory to obtain certain upper bounds related to the non-trivial primitive solutions to $(\star)$.

Several methods are used in [38] and then are generalized in the present paper, including:

- **Theoretical mathematical methods**: (i) Primarily using slightly changed IUT theory, such as 2-torsion initial Θ-data, sharper effective abc inequalities over rational numbers and their applications to the generalised Fermat equations. (ii) A little from analytic number theory related to prime number theorem, for upper bounds related to solutions, cf. the estimation in [38], Section 2.3 for an example.

- **Computations using computers**: (i) Reducing upper bounds in many specific cases. For example, for $r, s, t \geq 8$ and positive primitive solutions (x, y, z) to $x^r + y^s = z^t$, let $h \stackrel{\text{def}}{=} \log(x^r y^s z^t)$. By using analytic number theory and effective abc inequalities, it is shown in [38], Theorem 4.4 that $h < C_0 \stackrel{\text{def}}{=} 10^6$. Then we can choose finitely concrete examples of S and k in [38], Lemma 4.3, to show that h does not belong to the interval $(600, C_0)$. As a result, we can deduce that $h \leq 600$. (ii) Searching for possible solutions via computer for large exponents, cf. [38], Corollary 4.6 for an example. In this paper, new algorithms based on thestructure of solutions are used to accelerating the speed of search.

It is worth noting that by choosing more concrete examples of S and k in [38], Lemma 4.3, we can show that h does not belong to the interval $(600, C_0)$ for arbitrary large $C_0 > 0$. Since we can always obtain a [possibly large] upper bound C_0 for h using analytic number theory, the value of C_0 is not the core of the proof. Therefore, we shall omit the process of proving "$h < C_0$" in the several cases in this paper, and claim that we can always do the similar things presented above to provide "a valid and rigorous full proof", cf. Remark 1.13.1 for a discussion about this.

The main results of the present paper are as following:

Theorem A. The generalized Fermat equation $x^r + y^s = z^t$ has no non-trivial primitive solution except for the Catalan solutions and the nine non-Catalan solutions enumerated earlier, when (r, s, t) does not correspond to any permutation of the following cases:

- $(4, 5, n)$, $(4, 7, n)$, $(5, 6, n)$, 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 $m \geq 5$, $n \geq 7$.

Corollary B. 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.

It is worth noting that Catalan's conjecture is used in this paper to get upper bounds for the exponents; with further analysis of upper bounds and more computations for searching solutions, an expanded set of signatures including the permutations of $(4, 7, n)$, $(5, 6, n)$ are likely to be solved.

The present paper is organized as follows. In Section 1, we make preparations for the application of IUT Theory in three aspects: the "2-torsion version" of IUT theory, the arithmetic of elliptic curves for the construction of initial Θ-data, and the procedure to deduce "upper bounds" from "partial inequalities". Such procedure is a generalization of the methods in [38].

In Sections 2-4, we research on the generalized Fermat equation ($\star$) with each of the above four cases of signatures, using some classes of [modified] Frey-Hellegouarch curves:

- For general signatures (r, s, t) with $r, s, t \geq 4$, the curve $Y^2 + XY = X^3 + \frac{b-a-1}{4} \cdot X^2 - \frac{ab}{16} \cdot X$, where (a, b, c) is a triple of non-zero coprime integers such that $a + b = c$, $4 \mid (a + 1)$ and $16 \mid b$, cf. Section 2 for details.
- For permutations of $(2, 3, t)$ with $t \geq 7$, the curve $Y^2 = X^3 + 3bX + 2a$, where (a, b, c) is a triple of non-zero coprime integers such that $a^2 + b^3 = c$, cf. Section 3 for details.
- For permutations of $(3, r, s)$ with $r \geq 3$, $s \geq 4$, the curve $Y^2 + 3cXY + aY = X^3$, where (a, b, c) is a triple of non-zero coprime integers such that $a + b = c^3$, cf. Section 4 for details.
- For permutations of $(2, r, s)$ with $r \geq 4$, $s \geq 5$, the curve $Y^2 = X^3 + 2cX^2 + aX$, where (a, b, c) is a triple of non-zero coprime integers such that $a + b = c^2$, the related work will be undertaken in future studies.

Section 5 is a summary of the conclusions.

Acknowledgements

The main results of the present paper were obtained during the author's stay at Westlake University from September 2024 to February 2025. In particular, the discussions with Ivan Fesenko and later with Shinichi Mochizuki about the reason of adding 3-torsion points in the definition of initial Θ-data were crucial to the completion of this paper. The author also benefited from the talks given by Arata Minamide, Emmanuel Lepage, and Preda Mihăilescu at Westlake University, which provided some inspiration for this work. The author is especially grateful to Ivan Fesenko for his encouragements, discussions, and support during his stay, which greatly surpassed the author's expectations regarding the support received.

0 Notations and Conventions

Numbers:

Let N be a non-zero integer, k be a positive integer. For each prime number p, write $v_p(N)$ for the p-adic valuation of N. The radical of N, denoted by $\mathrm{rad}(N)$, is the product of distinct prime divisors of N; we shall write $N_{(k)}$ for the "coprime to k part" of N, and write $N^{\langle k\rangle}$ for the product of $p^{v_p(N)}$ for all possible prime number p such that $v_p(N)$ is divided by k. Hence we have

$$\mathrm{rad}(N) \stackrel{\mathrm{def}}{=} \prod_{p:\, p|N} p, \quad N_{(k)} \stackrel{\mathrm{def}}{=} \prod_{p:\, p\nmid k} p^{v_p(N)}, \quad N^{\langle k\rangle} \stackrel{\mathrm{def}}{=} \prod_{p:\, k|v_p(N)} p^{v_p(N)}.$$

Let p be a prime number. We shall write $\mathbb{Q}$ (respectively, $\mathbb{R}$; $\mathbb{Q}_p$) for the field of rational numbers (respectively, real numbers; p-adic rational numbers), and write $\mathbb{Z}$ for the ring of rational integers. We shall call finite extension of $\mathbb{Q}$ number field, call finite extension of $\mathbb{Q}_p$ p-adic local field. We shall write $\mathbb{Z}_{\geq 1}$ for the set of positive integers.

Curves:

Let K be a field of characteristic zero with an algebraic closure $\overline{K}$, E be an elliptic curve defined over K, $n \geq 1$ be an positive integer. Then we shall write $E[n]$ for the group of n-torsion points of $E_{\overline{K}} \stackrel{\mathrm{def}}{=} E \times_K \overline{K}$, and write $K(E[n]) \subseteq \overline{K}$ for the "n-torsion point field" of E, i.e. the field generated by K and the coordinates of the points in $E[n]$.

Ramification Datasets:

Ramification dataset is a concept introduced in [38], Section 1.3, which encodes the ramification information of initial Θ-data. This concept will be used frequently in the present paper.

1 Preparations for IUT Theory Applications

1.1 2-torsion version of IUT theory

We shall introduce the concept of 2-torsion initial Θ-data.

Definition 1.1. We shall refer to 2-torsion initial Θ-data as any collection of data

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

satisfying the following conditions:

- [24], Definition 3.1, (a), (c), (d), (e), (f).
- The "2-torsion version" of [24], Definition 3.1, (b), i.e., the condition obtained by replacing, in [24], 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}".

Remark 1.1.1. It is worth noting that the results of [24, 25, 26, 27] 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 [24], Remark 3.1.5, [27], Theorem 1.10 and [27], Corollary 2.2 via [27], 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 [24], 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 $L = F_{\mathrm{mod}}(E[l])$, 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 $K = F(E_F[l]) = F \cdot L$ is Galois over F_{mod}.

The condition "$F(E[3]) = F$" is also used to show that E_F has a model over F_{mod} in [27], Theorem 1.10 and [27], 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 [24, 25, 26, 27] still hold for its 2-torsion version.

Remark 1.1.2. By applying Definition 1.1, the 2-torsion versions of Section 1.2 and Section 1.3 of [38] remains valid without essential changes, with the following exceptions:

(i) All the "μ_6-initial Θ-data" should be replaced by "2-torsion initial Θ-data".

(ii) In the 2-torsion version of [38], Lemma 1.6, the condition "$F = F(E_F[6])$" should be replaced by "$F = F(E_F[2])$", and the condition "$\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}} \subseteq \mathbb{V}^{\mathrm{non}}_{\mathrm{mod}}$ is a nonempty set of nonarchimedean valuations of F_{mod}" should be replaced by "$\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}} \subseteq \mathbb{V}^{\mathrm{non}}_{\mathrm{mod}}$ is a nonempty set of nonarchimedean valuations of F_{mod} of odd residue characteristic".

(iii) The proof of the 2-torsion version of [38], Proposition 1.9 follows from the discussion in Remark 1.1.1. Note that the 2-torsion version of [38], Corollary 1.13 also holds, since we only use the condition "$F = F(E_F[2])$" rather than the condition "$F = F(E_F[6])$" in the proof of [38], Corollary 1.13.

(iv) For a μ_6- or 2-torsion initial Θ-data $\mathfrak{D} = (\overline{F}/F, X_F, l, \underline{C}_K, \underline{\mathbb{V}}, \mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}, \underline{\epsilon})$ with $F_{\mathrm{mod}} = \mathbb{Q}$, we shall say $\mathfrak{D}$ is **of type (l, N, N')** if N is the denominator of the j-invarient of $j(E_F) \in F_{\mathrm{mod}} = \mathbb{Q}$, and $N' = \prod_{p:\, v_p \in \mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}} p^{\max\{0, v_p(N)\}}$.

Corollary 1.2. Let $\mathfrak{R}$ be a ramification dataset with base prime $l \geq 5$ and base index e_0. Then there exists an algorithm to compute a real number $\mathrm{Vol}(\mathfrak{R}) \geq 0$ that depends only on $\mathfrak{R}$, such that for any μ_6-initial Θ-data or 2-torsion initial Θ-data $\mathfrak{D}$ of type (l, N, N') admitting $\mathfrak{R}$, we have

$$\frac{1}{6}\log(N') \leq \frac{l^2+5l}{l^2+l-12} \cdot \left((1-\frac{1}{e_0 l}) \cdot \log \mathrm{rad}(N) - \frac{1}{e_0}(1-\frac{1}{l}) \log \mathrm{rad}(N^{\langle l \rangle})\right) + \mathrm{Vol}(\mathfrak{R}),$$

Proof. The corollary follows from [38], Corollary 1.13 and Remark 1.1.2, (iii). □

We shall also provide a 2-torsion version of [38], Proposition 2.5 as following.

Proposition 1.3. Let E be an elliptic curve defined over $\mathbb{Q}$ with j-invariant $j(E) \in \mathbb{Q}$; N be the denominator of $j(E)$; F be a number field which is Galois over $\mathbb{Q}$; $l \geq 5$ be a prime number such that $l \nmid [F : \mathbb{Q}]$; X_F be the punctured elliptic curve associated to $E_F \stackrel{\text{def}}{=} E \times_{\mathbb{Q}} F$. Suppose that:

(a) $\sqrt{-1} \in F$, $F(E[2]) = F$, E_F is semi-stable, and $F \subseteq \mathbb{Q}(E[n])$ for some positive integer $l \nmid n$.

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

(c) We have $l \geq 23$ and $l \neq 37, 43, 67, 163$; or E is semi-stable and $l \geq 11$; or N is not a power of 2, $l \geq 11$ and $l \neq 13$.

(d) We have $N'_{2l} \neq 1$, where $N'_{2l} \stackrel{\text{def}}{=} N_{(2l)}/N_{(2l)}^{\langle l \rangle} = \prod_{p:\, p \nmid 2l,\, l \nmid v_p(N)} p^{v_p(N)}$.

Then there exists a 2-torsion initial Θ-data

$$\mathfrak{D}(E, F, l, 2\text{-tor}) = (\bar{F}/F, X_F, l, \underline{C}_K, \underline{\mathbb{V}}, \mathbb{V}_{\text{mod}}^{\text{bad}}, \underline{\epsilon}),$$

with $\log(\mathfrak{q}) = \log(N'_{2l})$ [cf. the notation of the 2-torsion version of [38], Definition 1.7, (ii)].

Proof. By making use of the 2-torsion version of [38], Lemma 1.6, the proof of Proposition 1.3 is similar to the proof of [38], Proposition 2.5, except that we shall define $\mathbb{V}_{\text{mod}}^{\text{bad}} \stackrel{\text{def}}{=} \{v_p \in \mathbb{V}_{\mathbb{Q}}^{\text{non}} : p \nmid 2l,\ l \nmid v_p(N)\}$ and replace "N'_l" by "N'_{2l}". □

1.2 Arithmetic of elliptic curves

Lemma 1.4. Let p be a prime number, E be an elliptic curve defined over $\mathbb{Q}_p$ with j-invariant $j(E) \in \mathbb{Q}_p$. For each positive integer n, write $K_n \stackrel{\text{def}}{=} \mathbb{Q}_p(E[n])$, and write $e_p(n)$ for the ramification index of K_n over $\mathbb{Q}_p$.

(i) If $v_p(j(E)) \geq 0$, then E has potentially good reduction; if $v_p(j(E)) < 0$, then E has potentially multiplicative reduction; for each $n \geq 1$, we have $\mu_n \subseteq K_n$, and K_n is Galois over $\mathbb{Q}_p$, where μ_n represents the n-th roots of unity; for coprime integers m, n, we have $e_p(m), e_p(n) \mid e_p(mn)$, and $e_p(mn) \mid e_p(m) \cdot e_p(n)$.

(ii) We have $(p-1) \mid e_p(p)$ and $e_p(n) \mid \#\,\mathrm{GL}(2, \mathbb{Z}/n\,\mathbb{Z})$ for $n \geq 1$. If E has potentially good reduction, then for $n \geq 1$ such that $p \nmid n$, we have $e_2(n) \mid 24$ for $p = 2$; $e_3(n) \mid 12$ for $p = 3$, and $e_p(n) \mid 6$ for $p \geq 5$. If E has potentially multiplicative reduction, then for $n \geq 1$ such that $p \nmid n$, we have $e_p(n) \mid 2n$, $e_p(pn) \mid 2(p-1)n$ for $p \geq 2$, and $e_2(4n) \mid 8n$.

(iii) If $n \geq 3$ and $p \nmid n$, then $E_{K_n} \stackrel{\text{def}}{=} E \times_{\mathbb{Q}_p} K_n$ has semi-stable reduction, i.e. has good or multiplicative reduction.

(iv) If E has good reduction, then $e_p(p) \in \{p-1, p(p-1), p^2-1\}$, and for $p \nmid n$, we have $e_p(n) = 1$; if E has multiplicative reduction, then $e_p(p) = (p-1) \cdot p/\gcd(p, v_p(j(E))) \in \{p-1, p(p-1)\}$, and for $p \nmid n$, we have $e_p(n) = n/\gcd(n, v_p(j(E))) \mid n$.

Proof. For finite extension of p-adic local fields L/M, we shall write $e(L/M)$ for the ramification index of L over M.

For assertion (i), the results related to reduction type follows from the arithmetic of elliptic curves, cf. [34], Proposition 5.5 for a reference. Since $\gcd(m, n) = 1$, we have

$K_{mn} = \mathbb{Q}_p(E[mn]) = \mathbb{Q}_p(E[m], E[n]) = K_m \cdot K_n$, then the results related to ramification indices follows from algebraic number theory.

For assertion (ii), since $\mu_p \subseteq K_p$, we have $p - 1 = e(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p) \mid e_p(p)$; since $\mathrm{Gal}(K_n/\mathbb{Q}_p)$ is isomorphic to a subgroup of $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$, we have $e_p(p) \mid [K_n/\mathbb{Q}_p] \mid \#\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$. Now let n be a positive integer such that $p \nmid n$, and suppose that E has potentially good reduction. Then by [31], 5.6, there exists a finite extension L of the maximal unramified field extension $\mathbb{Q}_p^{\mathrm{ur}}$ of $\mathbb{Q}_p$, such that E has good reduction over L. Moreover, we have $[L : \mathbb{Q}_p^{\mathrm{ur}}] \mid 24$ if $p = 2$, $[L : \mathbb{Q}_p^{\mathrm{ur}}] \mid 12$ if $p = 3$, and $[L : \mathbb{Q}_p^{\mathrm{ur}}] \mid 6$ if $p \geq 5$. Then since $p \nmid n$, we have $e(L(E[n])/L) = 1$. Then $e_p(n) = e(K_n/\mathbb{Q}_p) = e(\mathbb{Q}_p^{\mathrm{ur}}(E[n])/\mathbb{Q}_p^{\mathrm{ur}}) \mid e(L(E[n])/\mathbb{Q}_p^{\mathrm{ur}}) = e(L/\mathbb{Q}_p^{\mathrm{ur}}) \mid [L : \mathbb{Q}_p^{\mathrm{ur}}]$, hence we have $e_p(n) \mid 24$ if $p = 2$, etc. The case that E has potentially multiplicative reduction can be proved similarly.

For assertion (iii), we only need to prove for the case when $n = p \geq 3$ is an odd prime number and for $n = 4$. For the case $n = p$, cf. [27], Proposition 1.8 (v). For the case $n = 4$, as is explained by Chris Wuthrich, we can prove by contradiction. Suppose that there exist E which has additive reduction over $K_n = \mathbb{Q}_p(E[4])$, let $\mathcal{E}$ be the Néron model of E over $\mathcal{O}_{K_n}$. Then sicne $p \nmid n = 4$, we have $p \geq 3$. By the Kodaira classification, the group of components of the Néron model $\mathcal{E}/\mathcal{O}_{K_n}$ cannot contain $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Therefore, we would have a point of order 2 in the identity component $\mathcal{E}^0(\mathcal{O}_{K_n})$. The reduction is additive, so the group of non-singular points is a p-group, which means that our 2-torsion point must belong to the kernel of reduction, i.e., the formal group. However the torsion subgroup of a formal group over $\mathcal{O}_{K_n}$ is also a p-group — a contradiction! This proves assertion (iii).

assertion (iv) is a reformulation of [38], Proposition 1.8, (iii) and (iv). □

For the convenience of description, we shall introduce some definitions.

Definition 1.5. Let E be an elliptic curve defined over $\mathbb{Q}$, and let F be a finite Galois field extension of $\mathbb{Q}$. Let $l \geq 5$ be a prime number, such that $l \nmid [F : \mathbb{Q}]$. For each prime number p, choose a place $\underline{v}$ of $K \overset{\mathrm{def}}{=} F(E[l])$ dividing p, and write $e_p(E, F, l)$ for the ramification index of $K_{\underline{v}}$ over $\mathbb{Q}_p$.

Remark 1.5.1. Since $\mathbb{Q}(E[l])$ is Galois over $\mathbb{Q}$ [cf. [1], Proposition 5.2.1 and Proposition 5.2.2] and F is Galois over $\mathbb{Q}$, we can see that K is Galois over $\mathbb{Q}$. Hence $e_p(E, F, l)$ is independent to the choice of $\underline{v}$, i.e. $e_p(E, F, l)$ is well-defined.

Corollary 1.6. Let E be an elliptic curve defined over $\mathbb{Q}$, such that E has semi-stable reduction at each $p \neq 2, 3$. Let N be the denominator of the j-invariant of E. Let $l \geq 5$ be a prime number, and we shall follow the notation of Definition 1.5.

Write $F \overset{\mathrm{def}}{=} \mathbb{Q}(E[12])$, $E_F \overset{\mathrm{def}}{=} E \times_{\mathbb{Q}} F$, and let w be a place of F with residue characteristic p. Then if $p \nmid N$, E_F has good reduction at w; if $p \mid N$, E_F has multiplicative reduction at w; we have $\sqrt{-1} \in F$, $2 \mid e_2(E, F, l)$, $2 \mid e_3(E, F, l)$ and $(l - 1) \mid e_l(E, F, l)$.

In the case of $p \nmid N$, we have $e_2(E, F, l) \mid 2^8 \cdot 3^2$ for $p = 2$, $e_3(E, F, l) \mid 2^6 \cdot 3^2$ for $p = 3$, $e_l(E, F, l) \in \{l - 1, l(l - 1), l^2 - 1\}$ for $p = l$, and $e_p(E, F, l) = 1$ for $p \neq 2, 3, l$.

In the case of $p \mid N$, we have $e_2(E, F, l) \mid 24l$ for $p = 2$, $e_3(E, F, l) \mid 48l$ for $p = 3$, $e_l(E, F, l) \mid 12l(l - 1)$ for $p = l$, and $e_p(E, F, l) \mid 12l$ for $p \neq 2, 3, l$.

Proof. We shall follow the notation of Definition 1.5 and prove via Lemma 1.4. Since 12-torsion points of E_F are defined over F, we can see that E_F has good [if $p \nmid N$] or multiplicative [if $p \mid N$] reduction at w, $\sqrt{-1} \in \mu_4 \subseteq \mathbb{Q}(E[4])$, and for $p \in \{2, 3, l\}$, we

have $(p-1) \mid e_p(E,F,l)$, cf. Lemma 1.4. Since $\mathbb{Q}(\sqrt{-1})$ only ramifies at 2, by Lemma 1.4, we have the following proof:

In the case of $p \nmid N$, for $p=2$, we have $e_2(E,F,l) \mid e_2(4) \cdot e_2(3l)$, which divides $\#\operatorname{GL}(2,\mathbb{Z}/4\mathbb{Z}) \cdot 24 = 2^8 \cdot 3^2$; for $p=3$, we have $e_3(E,F,l) \mid e_3(3) \cdot e_3(4l)$, which divides $\#\operatorname{GL}(2,\mathbb{Z}/3\mathbb{Z}) \cdot 12 = 2^6 \cdot 3^2$; for $p=l$, we have $e_l(E,F,l) = e_l(12l) = e_l(l) \in \{l-1, l(l-1), l^2-1\}$; and for $p \neq 2,3,l$, we have $e_p(E,F,l) = e_p(12l) = 1$.

In the case of $p \mid N$, for $p=2$, we have $e_2(E,F,l) = e_2(4 \cdot 3l) \mid 8 \cdot 3l = 24l$; for $p=3$, we have $e_3(E,F,l) = e_3(3 \cdot 4l) \mid 2 \cdot (3-1) \cdot 3 \cdot 4l = 48l$; for $p=l$, since E has multiplicative reduction at l, we have $e_l(E,F,l) = e_l(12l) \mid 12l(l-1)$; and for $p \neq 2,3,l$, since E has multiplicative reduction at p, we have $e_p(E,F,l) = e_p(12l) \mid 12l$. □

Corollary 1.7. Let (a,b,c) be a triple of non-zero coprime integers such that $a+b+c=0$, $4 \mid (a+1)$ and $16 \mid b$. Let E be the elliptic curve defined over $\mathbb{Q}$ by the equation

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

Let $l \geq 5$ be a prime number, and we shall follow the notation of Definition 1.5.

(i) E has semi-stable reduction [i.e. good or multiplicative reduction] at each p; $\mathbb{Q}(E[2]) = \mathbb{Q}$; the j-invariant of E is $j(E) = \frac{(a^2+ab+b^2)^3}{2^{-8}a^2b^2c^2}$, whose denominator N equals $2^{-8}a^2b^2c^2$.

(ii) Write $F \overset{\text{def}}{=} \mathbb{Q}(\sqrt{-1}, E[3])$, $E_F \overset{\text{def}}{=} E \times_{\mathbb{Q}} F$, and let w be a place of F with residue characteristic p. Then if $p \nmid N$, E_F has good reduction at w; if $p \mid N$, E_F has multiplicative reduction at w; we have $2 \mid e_2(E,F,l)$, $2 \mid e_3(E,F,l)$ and $(l-1) \mid e_l(E,F,l)$.

In the case of $p \nmid N$, we have $e_2(E,F,l) = 2$ for $p=2$, $e_3(E,F,l) \in \{2,6,8\}$ for $p=3$, $e_l(E,F,l) \in \{l-1, l(l-1), l^2-1\}$ for $p=l$, and $e_p(E,F,l) = 1$ for $p \neq 2,3,l$.

In the case of $p \mid N$, we have $e_2(E,F,l) \mid 6l$ for $p=2$, $e_3(E,F,l) \mid 6l$ for $p=3$, $e_l(E,F,l) \mid 3l(l-1)$ for $p=l$, and $e_p(E,F,l) \mid 3l$ for $p \neq 2,3,l$.

(iii) Write $F \overset{\text{def}}{=} \mathbb{Q}(\sqrt{-1})$, $E_F \overset{\text{def}}{=} E \times_{\mathbb{Q}} F$, and let w be a place of F with residue characteristic p. Then if $p \nmid N$, E_F has good reduction at w; if $p \mid N$, E_F has multiplicative reduction at w; we have $2 \mid e_2(E,F,l)$ and $(l-1) \mid e_l(E,F,l)$.

In the case of $p \nmid N$, we have $e_2(E,F,l) = 2$ for $p=2$, $e_l(E,F,l) \in \{l-1, l(l-1), l^2-1\}$ for $p=l$, and $e_p(E,F,l) = 1$ for $p \neq 2,l$.

In the case of $p \mid N$, we have $e_2(E,F,l) \mid 2l$ for $p=2$, $e_l(E,F,l) \mid l(l-1)$ for $p=l$, and $e_p(E,F,l) \mid l$ for $p \neq 2,l$.

Proof. For assertion (i), by using Tate's algorithm, we have

$$c_4(E) = a^2+ab+b^2, \quad \Delta(E) = 2^{-8}a^2b^2c^2, \quad j(E) = \frac{(a^2+ab+b^2)^3}{2^{-8}a^2b^2c^2}.$$

Since $\gcd(a,b,c) = 1$ and $16 \mid b$, we have $\gcd(c_4(E), \Delta) = 1$, hence E has semi-stable reduction at each p, and $N = 2^{-8}a^2b^2c^2$. Since E can also be defined by the equation $Y^2 = X(X-a)(X+b)$, we can see that the 2-torsion points of E are defined over $\mathbb{Q}$, hecne $\mathbb{Q}(E[2]) = \mathbb{Q}$.

For assertion (ii), we shall follow the notation of Definition 1.5 and prove via Lemma 1.4. Since E has semi-stable reduction at p, we can see that E_F has good [if $p \nmid N$] or multiplicative [if $p \mid N$] reduction at w, and for $p \in \{2,3,l\}$, we have $(p-1) \mid e_p(E,F,l)$, cf. Lemma 1.4.

In the case of $p \mid N$, since $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ only ramifies at 2, by Lemma 1.4, we have $e_2(E,F,l) \mid 2e_2(3l) \mid 6l$, $e_3(E,F,l) = e_3(3l) = e_3(l) \in \{2,6,8\}$, $e_l(E,F,l) = e_l(3l) = e_l(l) \in \{l-1, l(l-1), l^2-1\}$, and for $p \neq 2,3,l$, $e_p(E,F,l) = e_p(3l) = 1$.

Other cases in assertions (ii) and (iii) can be proved using a similar approach. □

Corollary 1.8. Let (a, b, c) be a triple of non-zero coprime integers such that $a^2 + b^3 = c$. Let E be the elliptic curve defined over $\mathbb{Q}$ by the equation

$$Y^2 = X^3 + 3bX + 2a,$$

Let $l \geq 5$ be a prime number, and we shall follow the notation of Definition 1.5.

(i) E has semi-stable reduction at each $p \neq 2, 3$; the j-invariant of E is $j(E) = \frac{1728b^3}{c}$, whose denominator N equals $|c|/\gcd(1728, c)$.

(ii) Suppose that $q \geq 5$ is a prime number, such that $q \neq l$ and $|c|^{1/q} \in \mathbb{Z}$. Write $F \overset{\text{def}}{=} \mathbb{Q}(\sqrt{-1}, E[2q])$, $E_F \overset{\text{def}}{=} E \times_{\mathbb{Q}} F$, and let w be a place of F with residue characteristic p. Then if $p \nmid N$, E_F has good reduction at w; if $p \mid N$, E_F has multiplicative reduction at w; we have $2 \mid e_2(E, F, l)$, $(q-1) \mid e_q(E, F, l)$ and $(l-1) \mid e_l(E, F, l)$.

In the case of $p \nmid N$, we have $e_2(E, F, l) \mid 2^5 \cdot 3^2$ for $p = 2$, $e_q(E, F, l) \in \{q-1, q(q-1), q^2-1\}$ for $p = q$, $e_l(E, F, l) \in \{l-1, l(l-1), l^2-1\}$ for $p = l$, and $e_p(E, F, l) = 1$ when $p \neq 2, q, l$.

In the case of $p \mid N$, we have $e_2(E, F, l) \mid 8ql$ for $p = 2$, $e_q(E, F, l) \mid 2ql(q-1)$ for $p = q$, $e_l(E, F, l) \mid 2l(l-1)$ for $p = l$, and $e_p(E, F, l) \mid 2ql$ for $p \neq 2, q, l$.

Proof. For assertion (i), by using Tate's algorithm, we have

$$c_4(E) = -144b, \quad \Delta(E) = -1728c, \quad j(E) = \frac{1728b^3}{c}.$$

Since $\gcd(a, b, c) = 1$, we have $\gcd(c_4(E), \Delta) = \gcd(1728, c)$, hence E has semi-stable reduction at each $p \neq 2, 3$, and $N = |c|/\gcd(1728, c)$.

For assertion (ii), the proof follows a similar approach to those of Corollary 1.6 and Corollary 1.7. □

Corollary 1.9. Let (a, b, c) be a triple of non-zero coprime integers such that $a + b = c^3$. Let E be the elliptic curve defined over $\mathbb{Q}$ by the equation

$$Y^2 + 3cXY + aY = X^3,$$

Let $l \geq 5$ be a prime number, and we shall follow the notation of Definition 1.5.

(i) E has semi-stable reduction at each $p \neq 3$; the j-invariant of E is $j(E) = \frac{27c^3(a+9b)^3}{a^3b}$, whose denominator N equals $|a^3b|/\gcd(27, a^3b)$.

(ii) Write $F \overset{\text{def}}{=} \mathbb{Q}(E[4])$, $E_F \overset{\text{def}}{=} E \times_{\mathbb{Q}} F$, and let w be a place of F with residue characteristic p. Then if $p \nmid N$, E_F has good reduction at w; if $p \mid N$, E_F has multiplicative reduction at w; we have $\sqrt{-1} \in F$, $2 \mid e_2(E, F, l)$ and $(l-1) \mid e_l(E, F, l)$.

In the case of $p \nmid N$, we have $e_2(E, F, l) \mid 96$ for $p = 2$, $e_3(E, F, l) \mid 12$ for $p = 3$, $e_l(E, F, l) \in \{l-1, l(l-1), l^2-1\}$ for $p = l$, and $e_p(E, F, l) = 1$ for $p \neq 2, 3, l$.

In the case of $p \mid N$, we have $e_2(E, F, l) \mid 8l$ for $p = 2$, $e_3(E, F, l) \mid 8l$ for $p = 3$, $e_l(E, F, l) \mid 4l(l-1)$ for $p = l$, and $e_p(E, F, l) \mid 4l$ for $p \neq 2, 3, l$.

Proof. For assertion (i), by using Tate's algorithm, we have

$$c_4(E) = 9c(a+9b), \quad \Delta(E) = 27a^3b, \quad j(E) = \frac{27c^3(a+9b)^3}{a^3b}.$$

Since $\gcd(a, b, c) = 1$, we have $\gcd(c_4(E), \Delta) = \gcd(27, a^3b)$, hence E has semi-stable reduction at each $p \neq 3$, and $N = |a^3b|/\gcd(27, a^3b)$.

For assertion (ii), the proof follows a similar approach to those of Corollary 1.6 and Corollary 1.7. □

Corollary 1.10. Let (a, b, c) be a triple of non-zero coprime integers such that $a + b = c^2$. Let E be the elliptic curve defined over $\mathbb{Q}$ by the equation

$$Y^2 = X^3 + 2cX^2 + aX,$$

Let $l \geq 5$ be a prime number, and we shall follow the notation of Definition 1.5.

(i) E has semi-stable reduction at each $p \neq 2$; the j-invariant of E is $j(E) = \frac{64(a+4b)^3}{a^2b}$, whose denominator N equals $|a^2b|/\gcd(64, a^2b)$.

(ii) Write $F \stackrel{\text{def}}{=} \mathbb{Q}(\sqrt{-1}, E[6])$, $E_F \stackrel{\text{def}}{=} E \times_{\mathbb{Q}} F$, and let w be a place of F with residue characteristic p. Then if $p \nmid N$, E_F has good reduction at w; if $p \mid N$, E_F has multiplicative reduction at w; we have $\sqrt{-1} \in F$, $2 \mid e_2(E, F, l)$, $2 \mid e_3(E, F, l)$ and $(l-1) \mid e_l(E, F, l)$.

In the case of $p \nmid N$, we have $e_2(E, F, l) \mid 2^5 \cdot 3^2$ for $p = 2$, $e_3(E, F, l) \mid 2^6 \cdot 3^2$ for $p = 3$, $e_l(E, F, l) \in \{l-1, l(l-1), l^2-1\}$ for $p = l$, and $e_p(E, F, l) = 1$ for $p \neq 2, 3, l$.

In the case of $p \mid N$, we have $e_2(E, F, l) \mid 24l$ for $p = 2$, $e_3(E, F, l) \mid 12l$ for $p = 3$, $e_l(E, F, l) \mid 6l(l-1)$ for $p = l$, and $e_p(E, F, l) \mid 6l$ for $p \neq 2, 3, l$.

Proof. For assertion (i), by using Tate's algorithm, we have

$$c_4(E) = 16(a + 4b), \quad \Delta(E) = 64a^2b, \quad j(E) = \frac{64(a+4b)^3}{a^2b}.$$

Since $\gcd(a, b, c) = 1$, we have $\gcd(c_4(E), \Delta) = \gcd(64, a^2b)$, hence E has semi-stable reduction at each $p \neq 2$, and $N = |a^2b|/\gcd(64, a^2b)$.

For assertion (ii), the proof follows a similar approach to those of Corollary 1.6 and Corollary 1.7. □

1.3 Applications of local inequalities

We shall talk about a modified version of the methods of [38], Lemma 3.1. We shall first introduce some symbols and the conditions they should satisfy. All necessary symbols [i.e. the symbols that need to be defined when applying the conclusions in this subsection] are marked in bold.

Definition 1.11. Throughout this section, we will use the following notation:

(a) Let $\boldsymbol{N, n_0, u_0, p_N}$ be positive integers, such that $v_p(n_0 \cdot N) \geq u_0$ and $p \geq p_N$ for each $p \mid N$. For each prime number l, write $N_l \stackrel{\text{def}}{=} \prod_{p:l|v_p(N)} p^{v_p(N)}$.

(b) Let $\boldsymbol{S}$ be a finite set of prime numbers ≥ 5, with cardinality $n \geq 2$; let $2 \leq \boldsymbol{k} \leq n$, $\boldsymbol{n_1(S), n_k(S)}$ be positive integers, $\boldsymbol{S_1}$ be a finite set of prime numbers; write p_0 for the sallest prime number in S, and write $k(S)$ for the product of the k smallest prime numbers in S.

Suppose that for each prime $p \in B \setminus S_1$ [for the definition of B, cf. (e)], we have $v_p(N) \geq n_1(S)$; for any k distinct prime numbers $l_1, ..., l_k \in S$ and each prime p, if $l_i \mid v_p(N)$ for $1 \leq i \leq k$, then $v_p(N) \geq n_k(S)$.

(c) Let $\boldsymbol{\lambda} > 0$ be a real number. For each $l \in S$, suppose that we have real numbers $\boldsymbol{\mathrm{Vol}(l)} \geq 0$, $\boldsymbol{a_1(l) \geq a_4(l)} > 0$, such that

$$\frac{1}{\lambda} \log(l^{-v_l(N)} \cdot N/N_l) \leq a_1(l) \cdot \log \mathrm{rad}(N) - a_4(l) \cdot \log \mathrm{rad}(N_l) + \mathrm{Vol}(l) \tag{1.1}$$

(Optional) In the present paper, if not otherwise specified, we shall take $\lambda = 6$; instead of defining $a_1(l)$, $a_4(l)$, we shall fix a positive integer $\boldsymbol{e_0}$, and write

$$a_1(l) \stackrel{\text{def}}{=} \frac{l^2 + 5l}{l^2 + l - 12} \cdot (1 - \frac{1}{e_0 l}), \; a_4(l) \stackrel{\text{def}}{=} \frac{l^2 + 5l}{l^2 + l - 12} \cdot \frac{1}{e_0}(1 - \frac{1}{l}).$$

(d) **(Optional)** Let $\boldsymbol{u_0'} \geq u_0$ be a positive integer, $\boldsymbol{P}$ be a subset of prime numbers, such that for each $p \in P$, if $p \mid N$, then $v_p(n_0 N) \geq u_0'$. Let $\boldsymbol{n_1'(S)} \geq n_1(S)$ be a positive integer, such that for each $p \in B' \setminus S_1$ [for the definition of B', cf. (e)], we have $v_p(N') = v_p(N) \geq n_1'(S)$.

(e) We shall write

$$A \overset{\text{def}}{=} \{p \in S : p \mid N\},\ B \overset{\text{def}}{=} \{p \mid N : \exists l \in S,\, l \mid v_p(N)\},\ C \overset{\text{def}}{=} \{p \mid N : p \notin (A \cup B)\},$$

$$A' \overset{\text{def}}{=} P \cap A,\ B' \overset{\text{def}}{=} P \cap B,\ C' \overset{\text{def}}{=} P \cap C,\ N' \overset{\text{def}}{=} \prod_{p \in P} p^{v_p(N)},\ n_0' \overset{\text{def}}{=} \prod_{p \in P} p^{v_p(n_0)};\ N_A \overset{\text{def}}{=} \prod_{p \in A} p^{v_p(N)},$$

$$N_B \overset{\text{def}}{=} \prod_{p \in B} p^{v_p(N)},\ N_C \overset{\text{def}}{=} \prod_{p \in C} p^{v_p(N)},\ N_A' \overset{\text{def}}{=} \prod_{p \in A'} p^{v_p(N')},\ N_B' \overset{\text{def}}{=} \prod_{p \in B'} p^{v_p(N')},\ N_C' \overset{\text{def}}{=} \prod_{p \in C'} p^{v_p(N')};$$

$$a_1 \overset{\text{def}}{=} \frac{\lambda}{n} \sum_{l \in S} a_1(l),\ a_2 \overset{\text{def}}{=} \frac{\lambda}{n} \sum_{l \in S} \mathrm{Vol}(l),\ a_3 \overset{\text{def}}{=} \sum_{l \in S} \log(l),\ a_4 = \lambda \cdot \min_{l \in S}\{a_4(l)\},\ a_5 = \sum_{p \in S_1} \log(p);$$

$$b_1 \overset{\text{def}}{=} \max\{\frac{a_1}{u_0}, \frac{k}{n} + \frac{a_1 - a_4}{n_1(S)}\},\ b_1' \overset{\text{def}}{=} \max\{\frac{a_1}{u_0'}, \frac{k}{n} + \frac{a_1 - a_4}{n_1'(S)}\} \leq b_1,$$

$$b_2 \overset{\text{def}}{=} \frac{a_1}{u_0} \cdot \log(n_0) + a_2 + a_1 a_3 + (a_1 - a_4) a_5.$$

Lemma 1.12. Proceeding with the notation in Definition 1.11 and suppose that $\log(N) < n_k(S) \cdot \log(p_N)$.

(i) We have

$$\sum_{l \in S} v_l(N) \cdot \log(l) = \log(N_A),\ \sum_{p \in B} \log(p) \leq \sum_{l \in S} \log \mathrm{rad}(N_l),\ \sum_{p \in C} \log(p) \leq \frac{\log(n_0 N_C)}{u_0},$$

$$\sum_{l \in S} \log(N_l) \leq (k-1) \cdot \log(N_B),\ \sum_{p \in B} \log(p) \leq \frac{1}{n_1(S)} \cdot \log(N_B) + a_5,$$

$$\sum_{p \in B} \log(p) \leq \frac{1}{n_1(S)} \cdot \log(N_B / N_B') + \frac{1}{n_1'(S)} \cdot \log(N_B') + a_5'.$$

(ii) We have

$$\log(N) \leq a_1 \cdot \log \mathrm{rad}(N) - a_4 \sum_{p \in B} \log(p) + a_2 + \frac{k}{n}(\log(N) - \log(N_C)). \tag{1.2}$$

(iii) We have

$$\log(N) \leq a_1 \cdot \log \mathrm{rad}(N_C) + (\frac{k}{n} + \frac{a_1 - a_4}{n_1(S)})(\log(N) - \log(N_C)) + a_2 + a_1 a_3 + (a_1 - a_4) a_5.$$

(iv) We have

$$\begin{aligned}\log(N) \leq & a_1 \cdot \log \mathrm{rad}(N_C) + (\frac{k}{n} + \frac{a_1 - a_4}{n_1(S)})(\log(N/N') - \log(N_C/N_C')) \\ & + (\frac{k}{n} + \frac{a_1 - a_4}{n_1'(S)})(\log(N') - \log(N_C')) + a_2 + a_1 a_3 + (a_1 - a_4) a_5'.\end{aligned}$$

Proof. For assertion (i), by the definition of the set A, we have

$$\sum_{l \in S} v_l(N) \cdot \log(l) = \sum_{l : l \in S, l \mid N} v_l(N) \cdot \log(l) = \sum_{l \in A} v_l(N) \cdot \log(l) = \log(N_A).$$

By the definition of N_l and B, we have

$$\sum_{l\in S}\log\operatorname{rad}(N_l)=\sum_{l\in S}\sum_{p:p|N,l|v_p(N)}\log(p)=\sum_{p\in B}\log(p)\cdot\Big(\sum_{l:l\in S,l|v_p(N)}1\Big)\geq\sum_{p\in B}\log(p)$$

By the definition of N_l and B, we also have

$$\sum_{l\in S}\log(N_l)=\sum_{l\in S}\sum_{p:p|N,l|v_p(N)}v_p(N)\cdot\log(p)=\sum_{p\in B}v_p(N)\cdot\log(p)\cdot\Big(\sum_{l:l\in S,l|v_p(N)}1\Big).$$

By the definition of n_0 and u_0, for each $p\in C$, we have $v_p(n_0\cdot N)\geq u_0$, hence

$$\begin{aligned}\sum_{p\in C}\log(p)\leq&\frac{1}{u_0}\sum_{p\in C}(v_p(n_0)+v_p(N))\cdot\log(p)\\ \leq&\frac{1}{u_0}\sum_{p\in C}v_p(N)\cdot\log(p)+\frac{1}{u_0}\sum_{p}v_p(n_0)\cdot\log(p)=\frac{\log(n_0N_C)}{u_0}.\end{aligned}$$

Now for each prime number $p\in B$, we claim that $\sum_{p:p\in S,p|v_l(N)}1\leq k-1$, which can be proved by contradiction as follows. Assume that $l_1,\ldots,l_k\in S$ are k distinct prime numbers, such that $l_i\mid v_l(N)$ for $1\leq i\leq k$. Then by the definition of $n_k(S)$, we have $v_p(N)\geq n_k(S)$, hence

$$\log(N)=\log(N)\geq v_p(N)\cdot\log(p)\geq n_k(S)\cdot\log(p_N)>\log(N).$$

— a contradiction. Thus the claim is true, hence we have

$$\begin{aligned}\sum_{l\in S}\log(N_l)=&\sum_{p\in B}v_p(N)\cdot\log(p)\cdot\Big(\sum_{l:l\in S,l|v_p(N)}1\Big)\\ \leq&(k-1)\cdot\sum_{p\in B}v_p(N)\cdot\log(p)=(k-1)\cdot\log(N_B).\end{aligned}$$

By the definition of $n_1(S)$ and $n_1(p)$, we have $\log(p)\leq\frac{1}{n_1(S)}\cdot v_p(N)\cdot\log(p)$ for each $p\in B\setminus S_1$, and $\frac{n_1(p)}{n_1(S)}\cdot\log(p)\leq\frac{1}{n_1(S)}\cdot v_p(N)\cdot\log(p)$ for each $p\in B\cap S_1$. Hence

$$\begin{aligned}\sum_{p\in B}\log(p)\leq&\frac{1}{n_1(S)}\cdot\sum_{p\in B}v_p(N)\cdot\log(p)+\sum_{p\in B\cap S_1}(1-\frac{n_1(p)}{n_1(S)})\cdot\log(p)\\ \leq&\frac{1}{n_1(S)}\cdot\log(N_B)+a_5.\end{aligned}$$

Similarly, we have

$$\sum_{p\in B}\log(p)\leq\frac{1}{n_1(S)}\cdot\log(N_B/N_B')+\frac{1}{n_1'(S)}\cdot\log(N_B')+a_5.$$

This proves assertion (i).

Next, we consider assertion (ii). By (1.1) we have

$$\log(N)\leq\lambda a_1(l)\cdot\log\operatorname{rad}(N)-\lambda a_4(l)\cdot\log\operatorname{rad}(N_l)+\lambda\operatorname{Vol}(l)+\log(N_l)+v_l(N)\cdot\log(l).\quad(1.3)$$

Then by taking the average of (1.3) for $l\in S$ and by assertion (i), we have

$$\begin{aligned}\log(N)\leq&a_1\log\operatorname{rad}(N)-a_4\sum_{l\in S}\log\operatorname{rad}(N_l)+a_2+\frac{1}{n}\sum_{l\in S}\log(N_l)+\frac{1}{n}\sum_{l\in S}v_l(N)\cdot\log(l)\\ \leq&a_1\log\operatorname{rad}(N)-a_4\sum_{p\in B}\log(p)+a_2+\frac{1}{n}(\log(N_A)+(k-1)\log(N_B)).\end{aligned}$$

Then since $\log(N_A), \log(N_B) \leq \log(N) - \log(N_C)$ by the fact $A \cap C = B \cap C = \emptyset$, we have

$$\log(N) \leq a_1 \log \operatorname{rad}(N) - a_4 \sum_{p \in B} \log(p) + a_2 + \frac{k}{n}(\log(N) - \log(N_C)).$$

This proves assertion (ii).

For assertion (iii), by the definition of A, B and C, for each $p \mid N$, we have $p \in A \cup B \cup C \subseteq S \cap B \cap C$, hence by (i) we have (note that $a_1 \geq a_4$ by definitinon)

$$\begin{aligned} &a_1 \log \operatorname{rad}(N) - a_4 \sum_{p \in B} \log(p) \leq a_1 \sum_{p \in S} \log(p) + (a_1 - a_4) \sum_{p \in B} \log(p) + a_1 \sum_{p \in C} \log(p) \\ \leq &a_1 a_3 + (a_1 - a_4)(\frac{\log(N_B)}{n_1(S)} + a_5) + a_1 \sum_{p \in C} \log(p). \end{aligned}$$

Then by (1.2) and $\log(N_B) \leq \log(N) - \log(N_C)$ we have

$$\begin{aligned} &\log(N) \leq a_1 \log \operatorname{rad}(N) - a_4 \sum_{p \in B} \log(p) + a_2 + \frac{k}{n}(\log(N) - \log(N_C)) \\ \leq &a_1 a_3 + (a_1 - a_4)(\frac{\log(N_B)}{n_1(S)} + a_5) + a_1 \sum_{p \in C} \log(p) + a_2 + \frac{k}{n}(\log(N) - \log(N_C)) \\ \leq &a_1 \cdot \log \operatorname{rad}(N_C) + (\frac{k}{n} + \frac{a_1 - a_4}{n_1(S)})(\log(N) - \log(N_C)) + a_2 + a_1 a_3 + (a_1 - a_4) a_5. \end{aligned}$$

This proves assertion (iii).

The proof of assertion (iv) is similar to the proof of assertion (iii), where we shall make use of $\sum_{p \in B} \log(p) \leq \frac{1}{n_1(S)} \cdot \log(N_B/N'_B) + \frac{1}{n'_1(S)} \cdot \log(N'_B) + a_5$ by (i), and $\log(N_B/N'_B) \leq \log(N/N') - \log(N_C/N'_C)$, $\log(N'_B) \leq \log(N') - \log(N'_C)$ by the fact $(B \setminus B') \cap (C \setminus C') = B' \cap C' = B \cap C = \emptyset$. □

Proposition 1.13. Proceeding with the notation in Definition 1.11 and suppose that $\log(N) < n_k(S) \cdot \log(p_N)$.

(i) Suppose that $b_1 < 1$, then we have

$$(1 - b_1) \cdot \log(N) \leq b_2. \tag{1.4}$$

Hence if $n_k(S) \cdot \log(p_N) > \frac{b_2}{1 - b_1}$, then $\log(N)$ cannot belong to the interval

$$(\frac{b_2}{1 - b_1}, n_k(S) \cdot \log(p_N)).$$

(ii) Suppose that $b_1 \leq 1$, $b'_1 < 1$, then we have

$$(1 - b'_1) \cdot \log(N') \leq b_2.$$

Hence if $n_k(S) \cdot \log(p_N) > \frac{b_2}{1 - b'_1}$, then $\log(N')$ cannot belong to the interval

$$(\frac{b_2}{1 - b'_1}, n_k(S) \cdot \log(p_N)).$$

Proof. For assertion (i), recall that by Lemma 1.12, (i) we have

$$\log \mathrm{rad}(N_C) = \sum_{p \in C} \log(p) \leq \frac{1}{u_0} \cdot \log(n_0 N_C).$$

Then by Lemma 1.12, (iii) and the definition of b_1, b_2, we have

$$\begin{aligned}\log(N) \leq & \frac{a_1}{u_0} \cdot \log(n_0 N_C) + (\frac{k}{n} + \frac{a_1 - a_4}{n_1(S)})(\log(N) - \log(N_C)) + a_2 + a_1 a_3 + (a_1 - a_4) a_5 \\ = & \frac{a_1}{u_0} \cdot \log(N_C) + (\frac{k}{n} + \frac{a_1 - a_4}{n_1(S)})(\log(N) - \log(N_C)) + b_2 \\ \leq & b_1 \cdot \log(N) + b_2.\end{aligned}$$

Hence we must have (1.4), and then assertion (i) follows.

For assertion (ii), similar to the proof of assertion (i), by Lemma 1.12, (i) and (iv) we have

$$\begin{aligned}\log(N) \leq & a_1 \cdot \log \mathrm{rad}(N_C/N'_C) - \frac{a_1}{u_0} \log(n_0/n'_0) + (\frac{k}{n} + \frac{a_1 - a_4}{n_1(S)})(\log(N/N') - \log(N_C/N'_C)) \\ & + a_1 \cdot \log \mathrm{rad}(N'_C) - \frac{a_1}{u'_0} \log(n'_0) + (\frac{k}{n} + \frac{a_1 - a_4}{n'_1(S)})(\log(N') - \log(N'_C)) + b_2 \\ \leq & b_1 \cdot \log(N/N') + b'_1 \cdot \log(N') + b_2.\end{aligned}$$

Then since $b_1 \leq 1$, we must have $\log(N') \leq b'_1 \cdot \log(N') + b'_2$, and hence assertion (ii) follows. □

Remark 1.13.1. (i) Proposition 1.13 provides an algorithm to eliminate impossible value intervals of $\log(N)$ by choosing suitable n_0, N, u_0, p_N, $S, k, S_1, n_1(S), n_k(S)$, λ, e_0, $\mathrm{Vol}(l)$, $u'_0, P, n'_1(S)$, as defined in Definition 1.11. From a mathematically rigorous point of view, the value of $\mathrm{Vol}(l)$ is obtained by constructing general μ_6- or 2-torsion initial Θ-data and estimating the log-volume, and we shall prove $\log(N) \leq C_0$ for some explicit (but possibly very large) real number $C_0 > 0$ at first. Then by choosing finite many suitable and explicit S, k, $\mathrm{Vol}(l)$, etc., in Definition 1.11, we can apply Proposition 1.13 to show that $\log(N)$ can't belong to the interval (C, C_0), where $C > 0$ is a real number much smaller than C_0. Hence we can obtain a smaller upper bound $\log(N) \leq C$. Smaller upper bound for $\log(N')$ can be obtained similarly.

(ii) For an example for the procedure described in (i), cf. [38], Section 4. The step to show $\log(N) \leq C_0$ can be proved via estimation, and the step to show $\log(N) \notin (C, C_0)$ can be done by the computation via computer. In this paper, when we apply Proposition 1.13, we shall omit the step to show $\log(N) \leq C_0$ using analytic number theory.

Instead, we shall only choose finitely many suitable S, k, $\mathrm{Vol}(l)$, etc., in Definition 1.11 by constructing suitable μ_6- or 2-torsion initial Θ-data to define $\mathrm{Vol}(l)$, and compute the step to show $\log(N) \notin (C, C_1)$ [with C small and C_1 bigger] via computer.

We claim that it is always possible to show $\log(N) < C_0$ for some $C_0 > C_1$ by the procedure described in (i), and show $\log(N) \notin (C_1, C_0)$ by computing more special cases via Proposition 1.13. Hence we can deduce that $\log(N) \leq C$.

2 The general signatures

Let $r, s, t \geq 4$ be positive integers. In this section, we shall consider about the generalized Fermat equation $x^r + y^s = z^t$ with signature (r, s, t).

2.1 Upper bounds

Lemma 2.1. Let $r, s, t \geq 4$ 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 $l \geq 11$ be a prime number.

(i) 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

$$Y^2 = X(X - a)(X + b),$$

then the j-invariant

$$j(E) = \frac{(a^2 + ab + b^2)^3}{2^{-8}a^2b^2c^2} = \frac{(a^2 + ab + b^2)^3}{2^{-8}x^{2r}y^{2s}z^{2t}} \notin \{0, 2^6 \cdot 3^3, 2^2 \cdot 73^3 \cdot 3^{-4}, 2^{14} \cdot 31^3 \cdot 5^{-3}\}.$$

Write

$$N \stackrel{\text{def}}{=} 2^{-8}x^{2r}y^{2s}z^{2t},\ N_l \stackrel{\text{def}}{=} N^{\langle l \rangle},\ N_l' \stackrel{\text{def}}{=} (N/N_l)_{(l)},\ N_{2l}' \stackrel{\text{def}}{=} (N/N_l)_{(2l)}.$$

Then $x, y, z \geq 2$, N is the denominator of $j(E)$ and E is semi-stable.

(ii) Write $F \stackrel{\text{def}}{=} \mathbb{Q}(\sqrt{-1}, E[3])$, then when $N_l' \neq 1$, by the construction in [38], Proposition 2.5, there exists a μ_6-initial Θ-data $\mathfrak{D} = \mathfrak{D}(E, F, l, \mu_6)$ of type (l, N, N_l').

Let $\mathfrak{R}_l^{(1)}$ be the ramification dataset [cf. [38], Definition 1.12] consists of the following data:

$$l_0 = l,\ e_0 = 3,\ S_0 = \{2, 3, l\},\ S_{\text{gen}}^{\text{multi}} = \{1, 3, l, 3l\},\ S_2^{\text{good}} = \{2\},$$
$$S_2^{\text{multi}} = \{2, 6, 2l, 6l\},\ S_3^{\text{good}} = \{2, 6, 8\},\ S_3^{\text{multi}} = \{2, 6, 2l, 6l\},$$
$$S_l^{\text{good}} = \{l - 1, l(l-1), l^2 - 1\},\ S_l^{\text{multi}} = \{l - 1, 3(l-1), l(l-1), 3l(l-1)\}.$$

Let $\mathfrak{R}_l^{(2)}$ be the ramification dataset obtained by setting $S_l^{\text{good}} = \emptyset$ in the definition of $\mathfrak{R}_l^{(1)}$, i.e. the ramification dataset consists of the following data:

$$l_0 = l,\ e_0 = 3,\ S_0 = \{2, 3, l\},\ S_{\text{gen}}^{\text{multi}} = \{1, 3, l, 3l\},\ S_2^{\text{good}} = \{2\},$$
$$S_2^{\text{multi}} = \{2, 6, 2l, 6l\},\ S_3^{\text{good}} = \{2, 6, 8\},\ S_3^{\text{multi}} = \{2, 6, 2l, 6l\},$$
$$S_l^{\text{good}} = \emptyset,\ S_l^{\text{multi}} = \{l - 1, 3(l-1), l(l-1), 3l(l-1)\}.$$

Then $\mathfrak{D}$ admits $\mathfrak{R}_l^{(1)}$; and if $l \mid xyz$, then $\mathfrak{D}$ admits $\mathfrak{R}_l^{(2)}$. Hence we have

$$\frac{1}{6}\log(N_l') \leq \frac{l^2 + 5l}{l^2 + l - 12} \cdot \big((1 - \frac{1}{3l}) \cdot \log \mathrm{rad}(N) - \frac{1}{3}(1 - \frac{1}{l}) \log \mathrm{rad}(N_l)\big) + \mathrm{Vol}(l), \tag{2.1}$$

where we write $\mathrm{Vol}(l) \stackrel{\text{def}}{=} \mathrm{Vol}(\mathfrak{R}_l^{(1)})$ if $l \nmid xyz$, and write $\mathrm{Vol}(l) \stackrel{\text{def}}{=} \mathrm{Vol}(\mathfrak{R}_l^{(2)}) \leq \mathrm{Vol}(\mathfrak{R}_l^{(1)})$ if $l \mid xyz$. The above inequality holds for $N_l' = 1$.

(iii) Write $F \stackrel{\text{def}}{=} \mathbb{Q}(\sqrt{-1})$, then when $N_{2l}' \neq 1$, by the construction in Proposition 1.3, there exists a 2-torsion initial Θ-data $\mathfrak{D} = \mathfrak{D}(E, F, l, 2\text{-tor})$ of type (l, N, N_{2l}').

Let $\mathfrak{R}_l^{(3)}$ be the ramification dataset [cf. [38], Definition 1.12] consists of the following data:

$$l_0 = l,\ e_0 = 1,\ S_0 = \{2, l\},\ S_{\text{gen}}^{\text{multi}} = \{1, l\},\ S_2^{\text{good}} = \{2\},\ S_2^{\text{multi}} = \{2, 2l\},$$
$$S_l^{\text{good}} = \{l - 1, l(l-1), l^2 - 1\},\ S_l^{\text{multi}} = \{l - 1, l(l-1)\}.$$

Let $\mathfrak{R}_l^{(4)}$ be the ramification dataset obtained by setting $S_l^{\mathrm{good}} = \emptyset$ in the definition of $\mathfrak{R}_l^{(3)}$. Then $\mathfrak{D}$ admits $\mathfrak{R}_l^{(3)}$; and if $l \mid xyz$, then $\mathfrak{D}$ admits $\mathfrak{R}_l^{(4)}$. Hence we have

$$\frac{1}{6}\log(N_l') \leq \frac{l^2+5l}{l^2+l-12} \cdot (1-\frac{1}{l}) \cdot \log \mathrm{rad}(N/N_l) + \mathrm{Vol}(l), \tag{2.2}$$

where we write $\mathrm{Vol}(l) \overset{\mathrm{def}}{=} \mathrm{Vol}(\mathfrak{R}_l^{(3)})$ if $l \nmid xyz$, and write $\mathrm{Vol}(l) \overset{\mathrm{def}}{=} \mathrm{Vol}(\mathfrak{R}_l^{(4)}) \leq \mathrm{Vol}(\mathfrak{R}_l^{(3)})$ if $l \mid xyz$.

Proof. For assertion (i), since $r, s, t \geq 4$, we have $v_2(x^r y^s z^t) \geq 4$, hence (a, b, c) exists. Then by Corollary 1.7, we have $j(E) = \frac{(a^2+ab+b^2)^3}{2^{-8}a^2b^2c^2}$, N is the denominator of $j(E)$, and E is semi-stable. In addition, we have $x, y, z \geq 2$ by Catalan's conjecture.

For assertion (ii), since $j(E) \notin J$, E is semi-stable over $\mathbb{Q}$, $N_l' \neq 1$, E_F is semi-stable [cf. Corollary 1.10], $l \geq 11$, $F = \mathbb{Q}(\sqrt{-1}, E[12])$ is Galois over $\mathbb{Q}$ [cf. [38], Proposition 2.1], by the construction in [38], Proposition 2.5, there exists a μ_6-initial Θ-data $\mathfrak{D} = \mathfrak{D}(E, F, l, \mu_6)$ of type (l, N, N_l'). Then by Corollary 1.6, we can see that $\mathfrak{D}$ admits $\mathfrak{R}_l^{(1)}$, and $\mathfrak{D}$ admits $\mathfrak{R}_l^{(2)}$ when $l \mid N$ [which is equivlent to $l \mid xyz$], hence by Corollary 1.2 we have (4.1). Since the log-volume of a ramification dataset is non-negative, we have $\mathrm{Vol}(l) \geq 0$, hence (4.1) holds for $N_l' = 1$.

For assertion (iii), by using Corollary 1.7, (iii), and using Proposition 1.3 instead of [38], Proposition 2.5, assertion (iii) can be proved similarly to the proof of assertion (ii). □

Lemma 2.2. Let $r, s, t \geq 4$ 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 S be a finite set of prime numbers with cardinality $n = |S| \geq 2$, such that for each $l \in S$, we have $l \geq 11$; let $2 \leq k \leq S$ be a positive integer, p_0 be the smallest prime number in S, $k(S)$ be the product of k smallest prime numbers in S; let $n_0 = 2^8$, $N = n_0^{-1} x^{2r} y^{2s} z^{2t}$, $u_0 = 8$, $p_N = 2$, $e_0 = 3$, $S_1 = \{2\}$, $n_1(S) = 2p_0$, $n_k(S) = 2k(S)$; for each $l \in S$, write $\mathrm{Vol}(l) \overset{\mathrm{def}}{=} \mathrm{Vol}(\mathfrak{R}_l^{(1)})$, cf. Lemma 2.1, (ii). Suppose that one of the following situations is satisfied:

(a) Let $u_0' \geq u_0$ be a positive integer, $P \subseteq \{p : v_p(N) \geq u_0'\} \cup \{p : p \nmid N\}$, $n_1'(S) = \max\{u_0', 2p_0\}$. In particular, we can let $u_0' = u_0$, $P = \{p : p \mid N\}$, $n_0' = n_0$ and $N' = N$.

(b) Let $u_0' \geq u_0$ be a positive integer, $P \subseteq \{p : v_p(N) \geq u_0'\} \cup \{p : p \nmid N\}$, $n_1'(S) = \min\{v_p(N) : p \in B' \setminus S_1\}$ [for the definition of B', cf. Definition 1.5, (e)], $n_0' = 2^8$ if $2 \in P$ and $n_0' = 1$ if $2 \notin P$.

(c) In the situation of (b), suppose that $s \geq r \geq t$. If $l \nmid rst$ for each $l \in S$, then we can let $u_0' = 2t$, $n_1'(S) = u_0' p_0$, $P = \{p : p \mid xyz\}$, $N' = N$; if $l \nmid rs$ for each $l \in S$, then we can let $u_0' = 2r$, $n_1'(S) = u_0' p_0$, $P = \{p : p \mid xy\}$, $N' = (n_0')^{-1} x^{2r} y^{2s}$; if $l \nmid s$ for each $l \in S$, then we can let $u_0' = 2s$, $n_1'(S) = u_0' p_0$, $P = \{p : p \mid x\}$, $N' = (n_0')^{-1} y^{2s}$.

Then the assumptions in Definition 1.11 are satisfied, and we can define b_1, b_2, b_1'. Hence if $b_1 \leq 1$, $b_1' < 1$ and $n_k(S) \cdot \log(2) > \frac{b_2}{1-b_1'}$, then by Lemma 1.12, $\log(N')$ cannot belong to the interval $(\frac{b_2}{1-b_1'}, n_k(S) \cdot \log(2))$.

Proof. To show that the assumptions in Definition 1.11 are satisfied, we only need to check for the definitions of $u_0, n_1(S), n_k(S), u_0', n_1'(S)$. The check for u_0, u_0' is trivial, and we shall only check for $n_1(S)$, and check for $n_1'(S)$ in the second case of the situation of (c) as an example.

For each $p \in B$, there exists $l \in S$, such that $l \mid v_p(N)$. Since $l \geq 11$, and we have $2 \mid v_p(N)$ by the definition of N, we have $2l \mid v_p(N)$, hence $v_p(N) \geq 2l \geq 2p_0 = n_1(S)$. Thus $n_1(S)$ is well-defined.

In the second case of the situation of (c), for each $p \in B'$, $p \neq 2$, there exists $l \in S$, such that $l \mid v_p(N)$. Since $l \geq 11$, $l \nmid rs$, and $v_p(N)$ is a multiple of $2r$, $2s$ by the definition $P = \{p : p \mid xy\}$ and $N' = (n_0')^{-1}x^{2r}y^{2s}$, we can see that $v_p(N)$ is a multiple of $2rl$ or $2sl$, hence $v_p(N) \geq 2s \cdot l \geq u_0'p_0 = n_1'(S)$. Thus $n_1'(S)$ is well-defined. □

Lemma 2.3. Let $r, s, t \geq 4$ 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 S be a finite set of prime numbers with cardinality $n = |S| \geq 2$, such that for each $l \in S$, we have $l \geq 11$ and $l \nmid rst$; let $2 \leq k \leq S$ be a positive integer, p_0 be the smallest prime number in S, $k(S)$ be the product of k smallest prime numbers in S;

let $n_0 = 1$, $N \stackrel{\text{def}}{=} (x^{2r}y^{2s}z^{2t})_{(2)}$, $8 \leq u_0 = 8 \leq \min\{2r, 2s, 2t\}$, $p_N = 3$, $e_0 = 1$, $S_1 = \emptyset$, $n_1(S) = u_0 \cdot p_0$, $n_k(S) = u_0 \cdot k(s)$;

Suppose that one of the following situations is satisfied:

(a) Let $u_0' \geq u_0$ be a positive integer, $P \subseteq \{p : v_p(N) \geq u_0'\} \cup \{p : p \nmid N\}$, $n_1'(S) = \max\{u_0', 2p_0\}$. In particular, we can let $u_0' = \min\{3r, s\}$, $P = \{p : p \mid N\}$, $n_0' = n_0$ and $N' = N$.

(b) Let $u_0' \geq u_0$ be a positive integer, $P \subseteq \{p : v_p(N) \geq u_0'\} \cup \{p : p \nmid N\}$, $n_1'(S) = \min\{v_p(N) : p \in B' \setminus S_1\}$ [for the definition of B', cf. Definition 1.5, (e)], $n_0' = 27$ if $3 \in P$ and $n_0' = 1$ if $2 \notin P$.

(c) In the situation of (b), suppose that $s \geq r \geq t$. Then we can let $u_0' = 2t$, $P = \{p : p \mid N\}$, $N' = N$; or let $u_0' = 2r$, $P = \{p : p \mid xy\}$, $n_0' = \gcd(2^8, x^{2r}y^{2s})$ and $N' = (n_0')^{-1}x^{2r}y^{2s}$; or let $u_0' = 2s$, $P = \{p : p \mid y\}$, $n_0' = \gcd(2^8, y^{2s})$ and $N' \stackrel{\text{def}}{=} (n_0')^{-1}x^{2r}$.

Then the assumptions in Definition 1.11 are satisfied, and we can define b_1, b_2, b_1'. Hence if $b_1 \leq 1$, $b_1' < 1$ and $n_k(S) \cdot \log(3) > \frac{b_2}{1-b_1'}$, then by Lemma 1.12, $\log(N')$ cannot belong to the interval $(\frac{b_2}{1-b_1'}, n_k(S) \cdot \log(3))$.

Proof. The proof follows from Lemma 2.1 and is elementary, which is similar to the proof of Lemma 2.2. □

Proposition 2.4. Let $r, s, t \geq 4$ 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 $\delta_r, \delta_s \in \{\pm 1\}$. Assume without loss of generality that $s \geq r \geq t \geq 4$.

(i) Let $s_0 \geq 4$ be a positive integer. Suppose that $s_0 \leq t$, let $h = \log(x^r y^s z^t)$; or $s_0 \leq r$, let $h = \log(x^r y^s)$; or $s_0 \leq s$, let $h = \log(y^s)$; or for a fixed prime number p, let $s_0 = v_p(N)$, $h = \frac{1}{2}v_p(N) \cdot \log(p)$.

Then we have $h \leq 1693$ for $s_0 = 4$; $h < 864$ for $s_0 = 5$; $h < 668$ for $s_0 = 6$; $h < 571$ for $s_0 \geq 7$; and $h < 427.5$ for $s_0 \geq 600$. Hence $s = \max\{r, s, t\} \leq 616$.

(ii) Let $s_0 \geq 4$ be a positive integer. Suppose that $s_0 \leq t$, let $h = \log((x^r y^s z^t)_{(2)})$; or $s_0 \leq r$, let $h = \log((x^r y^s)_{(2)})$; or $s_0 \leq s$, let $h = \log((y^s)_{(2)})$; or for a fixed prime number $p \neq 2$, let $s_0 = v_p(N)$, $h = v_p(x^r y^s z^t) \cdot \log(p)$.

Then we have $h \leq 807$ for $s_0 = 4$; $h < 395$ for $s_0 = 5$; $h < 312$ for $s_0 = 6$; $h < 268$ for $s_0 \geq 7$.

Proof. For assertion (i), the upper bounds of h follow from Lemma 2.2 and the computation in [37], also cf. Remark 1.13.1. By Catalan's conjecture, we have $x, y, z \geq 2$. Note that if $s \geq 600$, then we have $2^s \leq h = \log(y^s) \leq 427.5$. Hence $s \leq 427.5/\log(2) < 617$, thus $s \leq 616$. For assertion (ii), the upper bounds of h follow from Lemma 2.3 and the computation in [37]. □

2.2 Structure of solutions

We shall analyze the structure of the solution (x, y, z) in more detail.

Lemma 2.5. Let $r, s, t \geq 4$ 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 $\delta_r, \delta_s \in \{\pm 1\}$.

For each prime number $p \geq 11$, denote [cf. Lemma 2.1]

$$a_1(p) \stackrel{\text{def}}{=} 3 \cdot \frac{p^2 + 5p}{p^2 + p - 12} \cdot (1 - \frac{1}{p}),$$
$$a_2(p) \stackrel{\text{def}}{=} \max\{3 \cdot \mathrm{Vol}(\mathfrak{R}_p^{(3)}) + a_1(p) \cdot \log(2), 3 \cdot \mathrm{Vol}(\mathfrak{R}_p^{(4)}) + a_1(p) \cdot \log(2p)\}.$$

Then $3 < a_1(p) \leq 4$, and we have $a_2(11) \leq 71$, $a_2(13) \leq 74$, $a_2(17) \leq 80$, $a_2(19) \leq 84$, $a_2(23) \leq 91.1$.

Let $l \geq 11$ be a prime number such that $l \nmid r$. Write uniquely

$$x = x_1 \cdot 2^{r_2} \cdot l^{r_l} \cdot x_l^l, \tag{2.3}$$

where $x_1, x_l, 2, l$ are pairwise coprime positive integers, $r_2, r_l \geq 0$, $x_l^l = x_{(2l)}^{\langle l \rangle}$.

(i) We have

$$a_2(l) \geq r \cdot \log(x_1) - a_1(l) \cdot \log \mathrm{rad}(x_1) \geq (r - 4) \cdot \log(x_1). \tag{2.4}$$

(ii) we have $x_l \in \{1, 3, 5\}$ if $(r, l) = (4, 11)$; $x_l \in \{1, 3\}$ if $(r, l) = (4, 13), (4, 17), (5, 11), (5, 13), (6, 11)$; and $x_1 = 1$ otherwise.

(iii) We have $r_l \leq \frac{37}{r}$. Hence if $r \geq 38$, then we have $r_l = 0$, $x_l = 1$, $x = x_1 \cdot 2^{r_2}$; if $r \geq 69$, then we further have $x_1 = 1$, $x = 2^{r_2}$.

(iv) Suppose that $l \nmid s$, write uniquely $y = y_1 \cdot 2^{s_2} \cdot l^{s_l} \cdot y_l^l$, where $y_1, y_l, 2, l$ are pairwise coprime, $s_2, s_l \geq 0$, $y_l^l = y_{(2l)}^{\langle l \rangle}$. Then we have $x_l = 1$ or $y_l = 1$.

Proof. For assertion (i), note that we have $\log \mathrm{rad}(N/N^{\langle l \rangle}) \leq \log \mathrm{rad}(N_{(2l)}/N_{(2l)}^{\langle l \rangle}) + \log(2)$ when $l \nmid xyz$, and $\log \mathrm{rad}(N/N^{\langle l \rangle}) \leq \log \mathrm{rad}(N_{(2l)}/N_{(2l)}^{\langle l \rangle}) + \log(2l)$ when $l \mid xyz$. Hence by (2.2) we have

$$\frac{1}{2} \log(N_{(2l)}/N_{(2l)}^{\langle l \rangle}) \leq a_1(l) \cdot \log \mathrm{rad}(N_{(2l)}/N_{(2l)}^{\langle l \rangle}) + a_2(l). \tag{2.5}$$

Since $l \nmid r$, by (2.3) we have $x_1^r \mid N_{(2l)}/N_{(2l)}^{\langle l\rangle}$. Then since $r, s, t \geq 4 \geq a_1(l)$, we have

$$\begin{aligned} a_2(l) &\geq \frac{1}{2}\log(N_{(2l)}/N_{(2l)}^{\langle l\rangle}) - a_1(l)\cdot \log \mathrm{rad}(N_{(2l)}/N_{(2l)}^{\langle l\rangle}) \\ &\geq \log(x_1^r) - a_1(l)\cdot \log\mathrm{rad}(x_1) + \sum_{p:p\mid yz, l\nmid v_p(y^s z^t)} (v_p(y^s z^t) - 4)\cdot \log(p) \\ &\geq r\cdot \log(x_1) - a_1(l)\cdot \log\mathrm{rad}(x_1). \end{aligned}$$

This proves assertion (i).

For assertion (ii), let q be the smallest prime number $q \geq 11$, such that $q \neq l$, $q \nmid r$ and $q \nmid x_l$. Write uniquely $x = x_1' \cdot 2^{r_2} \cdot q^{r_q} \cdot x_q^q$ similar to (2.3), where $x_1', x_q, 2, q$ are pairwise coprime, $r_2, r_q \geq 0$, $x_q^q = x_{(2q)}^{\langle q\rangle}$. Then by (2.4) we have $(r-4)\cdot \log\mathrm{rad}(x_1') \leq a_2(q)$.

Note that we have $\gcd(x_l, 2q) = 1$, and we claim that $\gcd(x_l, x_q) = 1$. In fact, suppose that we have $p \mid x_l$, $p \mid x_q$ for some prime p, then $p \geq 3$ and $ql \mid v_p(x)$ by definition. Hence by Proposition 2.4, we can take $s_0 \overset{\text{def}}{=} v_p(x) \geq rql > 100$, then $268 > h \overset{\text{def}}{=} v_p(x^r)\cdot \log(p) > rs_0 \cdot \log(3) > 4\cdot 100\cdot \log(3) > 400$ — a contradiction! Hence we have $\gcd(x_l, x_q) = 1$.

Since $x_l^l \mid x = x_1' \cdot 2^{r_2} \cdot q^{r_q} \cdot x_q^q$ and $\gcd(x_l, 2qx_q) = 1$, we can deduce that $x_l^l \mid x_1'$. Then by (i), $a_2(q) \geq r\cdot \log(x_1') - 4\log\mathrm{rad}(x_1') \geq (rl-4)\log(x_l)$, thus

$$\log(x_l) \leq \frac{a_2(q)}{rl-4}. \tag{2.6}$$

By Proposition 2.4 we have $268 \geq \log(x_l^{lr}) = lr\cdot\log(x_l) \geq 11r\cdot\log(x_l)$, hence $\log(x_l) \leq \frac{24.5}{r}$, $x_l \leq e^{24.5/r}$. Consider in the following cases.

(1) In the case of $r \geq 8$, we have $x_l \leq e^{25/r} \leq e^{25/8} < 30$. Then since $r \leq 616$ by Proposition 2.4, at most four of $11, 13, 17, 19, 23$ divide l, r or x_l. Hence we can deduce that $q \leq 23$, and $\log(x_l) \leq 92/(8\cdot 11 - 4) < \log(3)$ by 2.6, thus $x_1 < 3$. Then since x_1 is coprime to 2, we have $x_1 = 1$.

(2) In the case of $r \in \{5, 6, 7\}$, since $x_l \leq e^{24.5/r} \leq e^{24.5/5} < 140 < 11\cdot 13$, we can also deduce that $q \leq 17$. Hence by (2.6), we have $\log(x_l) \leq 80/(5\cdot 11 - 4) < \log(5)$, thus $x_1 < 5$. Then we can also deduce that $q \leq 13$.

When $l = 11$, we can take $q = 13$, and we have $x_l < 74/(7\cdot 11 - 4) < \log(3)$, $x_l = 1$ if $r = 7$; $x_l < 74/(5\cdot 11 - 4) < \log(5)$, $x_l \in \{1, 3\}$ if $r \in \{5, 6\}$. Similarly, if $l \geq 13$, we can take $q = 11$, and we have $x_l = 1$ if $r = 6$ or $l \geq 17$; $x_l \in \{1, 3\}$ if $r = 5$ and $l = 13$.

(3) In the case of $r = 4$, similar to the proof of case (2), we can first show that $x_l < 10$. Then we can deduce that $q \in \{11, 13\}$. When $l = 11$, we can take $q = 13$, hence $\log(x_l) \leq \frac{74}{rl-4} < \log(7)$, $x_l \in \{1, 3, 5\}$. Similarly, if $l \geq 13$, we can take $q = 11$, and we have $x_l = 1$ if $l \geq 19$; $x_l \in \{1, 3\}$ if $l \in \{13, 17\}$.

In conclusion, we have $x_l \in \{1, 3, 5\}$ if $(r, l) = (4, 11)$; $x_l \in \{1, 3\}$ if $(r, l) = (4, 13)$, $(4, 17)$, $(5, 11)$, $(5, 13)$, $(6, 11)$; and $x_1 = 1$ otherwise.

For assertion (iii), let q be the smallest prime number $q \geq 11$, such that $q \neq l$, $q \nmid r$ and $q \nmid r_l$. Write uniquely $x = x_1' \cdot 2^{r_2} \cdot q^{r_q} \cdot x_q^q$ similar to (2.4), where $x_1', x_q, 2, q$ are pairwise coprime, $r_2, r_q \geq 0$, $x_q^q = x_{(2q)}^{\langle q\rangle}$. Then by (2.4) we have $(rr_l - 4)\cdot\log(l) \leq r\cdot\log(x_1') - 4\log\mathrm{rad}(x_1') \leq a_2(q)$, thus

$$r_l \leq \frac{a_2(q)/\log(l) + 4}{r}. \tag{2.7}$$

Similar to the proof of assertion (ii), when $r \geq 100$, we can show that $q \leq 23$, $a_2(q) \leq 91.1$, hence by (2.7) we have $r_l < 1$, $r_l = 0$; when $r < 100$, we can show that

$q \le 19$ hence $r_l \le 10$, then we can show that $q \le 17$, $a_2(q) \le 80$, hence by (2.7) we have $r_l \le \frac{80/\log(l)+4}{r} < \frac{38}{r}$, thus $r_l \le \frac{37}{r}$. Then if $r \ge 38$, we have $r_l = 0$, $x_l = 1$, hence $x = x_1 \cdot 2^{r_2}$.

Suppose that $r \ge 69$, then $x = x_1 \cdot 2^{r_2}$, and for each prime number $p \ge 11$, $p \nmid r$, by (2.4) we have $\log(x_1) < a_2(p)/(r-4)$. If $11 \nmid r$, take $p = 11$, then we have $\log(x_1) < a_2(11)/(69-4) < \log(3)$, hence $x_1 = 1$; if $11 \mid r$ and $13 \nmid r$, then $r \ge 77$, take $p = 13$, then we have $\log(x_1) < a_2(13)/(77-4) < \log(3)$, hence $x_1 = 1$; if $11, 13 \mid r$, since $r \le 616$, we have $r > 100$, $17 \nmid r$, we can take $p = 17$, then $\log(x_1) < a_2(17)/(100-4) < \log(3)$, hence $x_1 = 1$. In summary, we have $x_1 = 1$, $x = 2^{r_2}$ for $r \ge 69$.

assertion (iv) can be proved by a similar approach to the proof of assertion (i). □

Lemma 2.6. Let $r, s, t \ge 4$ 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 $\delta_r, \delta_s \in \{\pm 1\}$.

For each prime number $p \ge 17$, write [cf. Lemma 2.1]

$$a_1(p) \overset{\text{def}}{=} 3 \cdot \frac{p^2+5p}{p^2+p-12} \cdot (1 - \frac{1}{3p}),$$
$$a_2(p) \overset{\text{def}}{=} \max\{3 \cdot \mathrm{Vol}(\mathfrak{R}_p^{(1)}) + a_1(p) \cdot \log(2), 3 \cdot \mathrm{Vol}(\mathfrak{R}_p^{(2)}) + a_1(p) \cdot \log(2p)\}.$$

Then $3 < a_1(p) < 4$, and we have $a_2(17) \le 156$, $a_2(19) \le 164$, $a_2(23) \le 182$, $a_2(29) \le 210$, $a_2(31) \le 219$, $a_2(37) \le 248$.

Write $r_2 \overset{\text{def}}{=} v_2(x)$. Let l be a prime number ≥ 17, such that $l \nmid rst$, $l \nmid (r_2 r - 4)$. Write uniquely

$$x = x_1 \cdot 2^{r_2} \cdot l^{r_l} \cdot x_l^l,\ y = y_1 \cdot 2^{s_2} \cdot l^{s_l} \cdot y_l^l,\ z = z_1 \cdot 2^{t_2} \cdot l^{t_l} \cdot z_l^l.$$

where $x_1, x_l, y_1, y_l, z_1, z_l, 2, l$ are pairwise coprime positive integers, $r_2, r_l, s_2, s_l, t_2, t_l \ge 0$, $x_l^l = x_{(2l)}^{\langle l \rangle}$, $y_l^l = y_{(2l)}^{\langle l \rangle}$, $z_l^l = z_{(2l)}^{\langle l \rangle}$.

(i) We have

$$v_2(x^r) = r_2 r \le (a_2(l) + 4 \log \mathrm{rad}(x_l y_l z_l))/\log(2) + 4. \tag{2.8}$$

(ii) We have $v_2(x^r) = r_2 r \le 306$, hence $r_2 \le \frac{306}{r}$. Moreover, we have $r \le 303$.

Proof. For assertion (i), since $a_2(l) \ge 0$, the right hand of (2.8) is ≥ 4, hence (2.8) is valid when $r_2 r \le 4$. Now we shall assume that $r_2 r > 4$. Then since $\gcd(x, y, z) = 1$ and $r_2 > 0$, we have $s_2 = t_2 = 0$.

When $l \mid xyz$, following the notation in Lemma 2.1 and (2.1), we have $l \nmid v_2(N) = 2(r_2 r - 4) > 0$, $N_l = (x_l^{2r} y_l^{2s} z_l^{2t})^l$, $N_l' = 2^{-8} x_1^{2r} y_1^{2s} z_1^{2t}$, $\log \mathrm{rad}(N) = \log \mathrm{rad}(2l x_1 y_1 z_1 x_l y_l z_l)$. Then by (2.1) we have

$$\log(x_1^r y_1^s z_1^t) \le a_1(l) \cdot \log \mathrm{rad}(N) + 3 \cdot \mathrm{Vol}(\mathfrak{R}_l^{(2)}) \le a_1(l) \cdot \log \mathrm{rad}(x_1 y_1 z_1 x_l y_l z_l) + a_2(l).$$

When $l \nmid xyz$, we have $\log \mathrm{rad}(N) = \log \mathrm{rad}(2 x_1 y_1 z_1 x_l y_l z_l)$. And we can prove $\log(x_1^r y_1^s z_1^t) \le a_1(l) \cdot \log \mathrm{rad}(x_1 y_1 z_1 x_l y_l z_l) + a_2(l)$ similarly.

Then since $a_1(l) < 4$, we have

$$\begin{aligned} a_2(l) + 4 \log \mathrm{rad}(x_l y_l z_l) &\ge \log(x_1^r y_1^s z_1^t) - a_1(l) \cdot \log \mathrm{rad}(x_1 y_1 z_1) \\ &\ge \sum_p (v_p(x_1^r y_1^s z_1^t) - 4) \cdot \log(p) \ge (r_2 r - 4) \cdot \log(2). \end{aligned}$$

This proves assertion (i).

For assertion (ii), recall that at most one of r, s, t equals to 4. Hence if $l = 17$, we have $x_l y_l z_l \in \{1, 3\}$; if $l \geq 19$, we have $x_l y_l z_l = 1$. Note that we have $a_2(17) + 4 \log \operatorname{rad}(x_l y_l z_l) \leq a_2(17) + 4 \log(3) < 160 < a_2(19)$.

We shall assume that each of s, t is divided by at most one prime number $p \geq 17$, because if we have $p \mid s$, then we can replace (y, s) by $(y^{s/p}, p)$. Similarly, if $r' \mid r$, $r' \geq 4$, then an upper bound of $v_2(x^r)$ when "$r = r'$" is also an upper bound of $v_2(x^r)$.

Since $r \geq 4$, note that by Proposition 2.4, we have $\log(2^{r_2 r}) \leq \log(x^r) \leq 1693$, hence $r_2 r \leq \frac{1693}{\log(2)} < 2443$, $r_2 r \leq 2442$. Moreover, let q be the smallest prime ≥ 17 such that $q \nmid rst$, $q \nmid (r_2 r - 4)$, then by (2.8), we have $r_2 r \leq (a_2(17) + 4 \log(3))/\log(2) + 4$ if $l = 17$, and $r_2 r \leq a_2(l)/\log(2) + 4$ if $l \geq 19$. Since there are only finitely many r, s, t, r_2, computation in [37] shows that we have $r_2 r \leq 306$, and we have $r_2 = 0$ if $r > 303$. However, if $r > 303$, then $r_2 = 0$ and we have $x = 1$ by Lemma 2.5. But by Catalan's conjecture we have $x \geq 2$ — a contradiction! Hence $r \leq 303$. This proves assertion (ii). □

Lemma 2.7. Let $r, s, t \geq 4$ 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 $\delta_r, \delta_s \in \{\pm 1\}$.

For each prime number $p \geq 11$, write [cf. Lemma 2.5]

$$a_1(p) \overset{\text{def}}{=} 3 \cdot \frac{p^2 + 5p}{p^2 + p - 12} \cdot (1 - \frac{1}{p}),$$
$$a_2(p) \overset{\text{def}}{=} \max\{3 \cdot \operatorname{Vol}(\mathfrak{R}_p^{(3)}) + a_1(p) \cdot \log(2), 3 \cdot \operatorname{Vol}(\mathfrak{R}_p^{(4)}) + a_1(p) \cdot \log(2p)\}.$$

Then $3 < a_1(p) \leq 4$, and we have $a_2(11) \leq 71$, $a_2(13) \leq 74$, $a_2(17) \leq 80$, $a_2(19) \leq 84$, $a_2(23) \leq 92$.

Let l be a prime number ≥ 11. Write uniquely

$$x = x_1 \cdot 2^{r_2} \cdot l^{r_l} \cdot x_l^l, \ y = y_1 \cdot 2^{s_2} \cdot l^{s_l} \cdot y_l^l, \ z = z_1 \cdot 2^{t_2} \cdot l^{t_l} \cdot z_l^l. \tag{2.9}$$

where $x_1, x_l, y_1, y_l, z_1, z_l, 2, l$ are pairwise coprime positive integers, $r_2, r_l, s_2, s_l, t_2, t_l \geq 0$, $x_l^l = x_{(2l)}^{\langle l \rangle}$, $y_l^l = y_{(2l)}^{\langle l \rangle}$, $z_l^l = z_{(2l)}^{\langle l \rangle}$. Write $r' \overset{\text{def}}{=} r - a_1(l)$, $s' \overset{\text{def}}{=} s - a_1(l)$, $t' \overset{\text{def}}{=} r - a_1(l)$.

(i) Suppose that $l \nmid rst$, then we have

$$r' \cdot \log(x_1) + s' \cdot \log(y_1) + t' \cdot \log(z_1) \leq a_2(l). \tag{2.10}$$

Hence

$$(r' + s') \cdot \min\{\log(x_1), \log(y_1)\} + t' \cdot \log(z_1) \leq a_2(l). \tag{2.11}$$

(ii) Suppose that $l \nmid rst$, and assume without loss of generality that $4 \leq r \leq s \leq t$. Then $t' \geq s' \geq 1$, $r' \geq 0$, and $r' = 0$ if and only if $(r, l) = (4, 11)$. Moreover, when $t' \leq r' + s'$, we have

$$\min\{\log(x_1 y_1), \log(x_1 z_1), \log(y_1 z_1)\} \leq \frac{2a_2(l)}{r' + s' + t'}. \tag{2.12}$$

(iii) Suppose that $l \nmid rs$, then we have

$$r' \cdot \log(x_1) + s' \cdot \log(y_1) \leq a_2(l), \quad \min\{\log(x_1), \log(y_1)\} \leq \frac{a_2(l)}{r' + s'}. \tag{2.13}$$

Proof. assertion (i) is consequence of Lemma 2.1. When $l \mid xyz$, following the notation in Lemma 2.1, we have $N_l = (x_l^{2r} y_l^{2s} z_l^{2t})^l$, $N_l' = x_1^{2r} y_1^{2s} z_1^{2t}$, $\log \operatorname{rad}(2^{-8} x^{2r} y^{2s} z^{2t}/N_l) \leq \log \operatorname{rad}(2l x_1 y_1 z_1)$. Then by (2.3) we have

$$\log(x_1^r y_1^s z_1^t) \leq a_1(l) \cdot \log \operatorname{rad}(2^{-8} x^{2r} y^{2s} z^{2t}/N_l) + 3 \cdot \operatorname{Vol}(\mathfrak{R}_l^{(4)}) \leq a_1(l) \cdot \log \operatorname{rad}(x_1 y_1 z_1) + a_2(l).$$

When $l \nmid xyz$, we have $\log \mathrm{rad}(2^{-8}x^{2r}y^{2s}z^{2t}/N_l) \le \log \mathrm{rad}(2x_1y_1z_1)$. Then we can prove $\log(x_1^r y_1^s z_1^t) \le a_1(l) \cdot \log \mathrm{rad}(x_1y_1z_1) + a_2(l)$ similarly.

Hence we have

$$\begin{aligned} a_2(l) &\ge \log(x_1^r y_1^s z_1^t) - a_1(l) \cdot \log(x_1y_1z_1) = r' \cdot \log(x_1) + s' \cdot \log(y_1) + t' \cdot \log(z_1) \\ &\ge (r'+s') \cdot \min\{\log(x_1), \log(y_1)\} + t' \cdot \log(z_1). \end{aligned}$$

This proves assertion (i).

For assertion (ii), since the signature $(2,4,n)$ or its permutation is solved for $n \ge 4$, we have $s,t \ge 5$, $3 < a_1(l) \le 4$, and $a_1(l) = 4$ if and only if $l = 11$. Hence $t' \ge s' \ge 1$, $r' \ge 0$, and $r' = 0$ if and only if $(r,l) = (4,11)$.

When $t' \le r'+s'$, to prove (2.12), let $A \overset{\text{def}}{=} \min\{\log(x_1y_1), \log(x_1z_1), \log(y_1z_1)\}$. Then by (2.10), we have $2a_2(l) \ge (r'+s'-t')\log(x_1y_1)+(r'+t'-s')\log(x_1z_1)+(s'+t'-r')\log(x_1y_1) \ge (r'+s'-t')A + (r'+t'-s')A + (s'+t'-r')A = (r'+s'+t')A$, hence $A \le \frac{2a_2(l)}{r'+s'+t'}$.

The proof of assertion (iii) is similar to that of assertion (i). □

Remark 2.8. (i) Suppose that $l \nmid rs$ and consider the unique decomposition $x = x_1 \cdot 2^{r_2} \cdot l^{r_l} \cdot x_l^l$. In Lemma 2.5 and Lemma 2.6, we have proved that $r \le 313$, $r_2 \le \frac{306}{r}$, $r_l \le \frac{37}{r}$; $x_l \in \{1,3,5\}$ if $(r,l) = (4,11)$, $x_l \in \{1,3\}$ if $(r,l) = (4,13), (4,17), (5,11), (5,13), (6,11)$, and $x_1 = 1$ otherwise. We have similar results for y [and for z if $l \nmid t$], and we have $x,y,z \ge 2$, $\min\{r_2,s_2,t_2\} = 0$, $\min\{r_l,s_l,t_l\} = 0$, $\min\{x_l,y_l\} = 1$. Combined with the upper bounds of x_1,y_1,z_1 in Lemma 2.7, we can try to search for all possible positive coprime integers (x,y,z) satisfying $\delta_r x^r + \delta_s y^s = z^t$, where $\delta_r, \delta_s \in \{\pm 1\}$.

(ii) To find all non-trivial primitive solutions of $x^r + y^s = z^t$, it suffices to find all possible positive coprime integers (x,y,z) satisfying $\delta_r x^r + \delta_s y^s = z^t$, where $\delta_r, \delta_s \in \{\pm 1\}$. Note that this equation is "symmetric" for r, s and t, hence we can assume without loss of generality that $4 \le r \le s \le t$. We shall apply the unique decomposition (2.9) to the possible solution (x,y,z), for prime number $l \ge 11$ chosen below.

When $l \nmid rst$ and any two of x_1,y_1,z_1 are given, suppose that x_1,y_1 are given as an example, then there are only finitelly many possible (x,y) [cf. the discussion in (i)]. To solve the equation $\delta_r x^r + \delta_s y^s = z^t$ with given (x_1,y_1), we only need to check whether $|x^r \pm y^s|$ is a t-th power for each possible (x,y,r,s,t). We shall call this procedure as check for (x_1,r,y_1,s,l,t).

When $t \ge 70$, we have $z = 2^{t_2}$, where $t_2 \ge 1$ [since $z \ge 2$] and $70 \le t \le t_2 t \le 306$ [since $t_2 \le \frac{306}{t}$]. If $s \ge 70$, then $y = 2^{s_2}$ is also even., which contradicts to $\gcd(x,y,z) = 1$, hence we have $4 \le r \le s < 70$. In the case of $t \ge 70$, when $l \nmid rs$ and any one of x_1,y_1 is given, suppose that y_1 is given as an example, then there are only finitelly many possible (y,z^t) [since $z^t = 2^m$, where $70 \le m \le 306$]. To solve the equation $\delta_r x^r + \delta_s y^s = z^t$ with given x_1, we only need to check whether $|y^s \pm 2^m|$ is a r-th power for each possible (y,m,r,s). We shall call this procedure as check for (x_1,r,l,s).

(iii) We can divide the search procedure into several parts:

(P1) For given $4 \le r \le s < 70$ and all possible $t \ge 70$, choose $l \in \{11,13,17,19\}$, $l \nmid rs$. Then by (2.13), we have $\min\{\log(x_1), \log(y_1)\} \le \frac{a_2(l)}{r'+s'}$. Then for $\log(x_1) \le \frac{a_2(l)}{r'+s'}$, check for (x_1,r,l,s); for $\log(y_1) \le \frac{a_2(l)}{r'+s'}$ (y_1,s,l,r).

(P2) For given $4 \le r \le s \le t < 70$ such that $t \ge r+s-3$, choose $l \in \{11,13,17,19\}$, $l \nmid rst$. Since $3 < a_1(l) \le 4$, we have $t' \ge r'+s'$. Then by (2.11), we have $(r'+s') \cdot \min\{\log(x_1), \log(y_1)\} + t' \cdot \log(z_1) \le a_2(l)$. Then for $(r'+s') \cdot \log(x_1) + t' \cdot$

$\log(z_1) \le a_2(l)$, check for (x_1, r, z_1, t, l, s); for $(r'+s')\cdot\log(y_1) + t'\cdot\log(z_1) \le a_2(l)$, check for (y_1, a, z_1, t, l, r).

(P3) For given $4 \le r \le s \le t < 70$ such that $t \le r+s-4$, choose $l \in \{11, 13, 17, 19\}$, $l \nmid rst$. Since $3 < a_1(l) \le 4$, we have $t' \le r'+s'$. Then by (2.12), we have $\min\{\log(x_1y_1), \log(x_1z_1), \log(y_1z_1)\} \le \frac{2a_2(l)}{r'+s'+t'}$. Then for $\log(x_1y_1) \le \frac{2a_2(l)}{r'+s'+t'}$, check for (x_1, r, y_1, s, l, t); for $\log(x_1z_1) \le \frac{2a_2(l)}{r'+s'+t'}$, check for (x_1, r, z_1, t, l, s); for $\log(y_1z_1) \le \frac{2a_2(l)}{r'+s'+t'}$, check for (y_1, s, z_1, t, l, r).

Proposition 2.9. For any integers $r, s, t \ge 4$, such that (r, s, t) is not a permutation of $(4, 5, n), (4, 7, n), (5, 6, n)$ with $7 \le n \le 301$, the generalized Fermat equation

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

has no non-trivial primitive solution.

Proof. It suffices to find all positive coprime integers (x, y, z) satisfying $\delta_r x^r + \delta_s y^s = z^t$, where $\delta_r, \delta_s \in \{\pm 1\}$. Note that this equation is "symmetric" for r, s and t, hence we can assume without loss of generality that $4 \le r \le s \le t$.

Then when $(r, s) \ne (4, 5), (4, 7), (5, 6)$, the computation in [38], which is based on the discussion in Remark 2.8 shows that such solution (x, y, z) does not exist.

When $(r, s) = (4, 5), (4, 7), (5, 6)$, by Lemma 2.6, we have $t \le 303$. Then since the signatures $(4, 5, 2), (4, 7, 2), (5, 6, 2), (4, 5, 3), (2, 7, 3), (5, 3, 3)$ have benn solved [cf. Introduction], t cannot divided by 2 or 3, hence $t \le 301$. We can prove $t \ge 7$ similarly. □

3 The signatures $(2, 3, t)$

Let $t \ge 7$ be a positive integer. In this section, we shall consider about the generalized Fermat equation with signature $(2, 3, t)$ or its permutations. Since the case of $t \in \{6, 7, 8, 9, 10, 15\}$ have been solved [cf. Introduction], we only need to consider for the case of $t \ge 11$ and $6, 7, 8, 9, 10, 15 \nmid t$. Then t must be a multiple of some prime number $q \ge 5$.

3.1 Upper bounds

Lemma 3.1. Let $t \ge 7$ be a positive integer, (x, y, z) be a triple of positive coprime integers such that $\delta_2 x^2 + \delta_3 y^3 = z^t$, where $\delta_2, \delta_3 \in \{\pm 1\}$. Write $z_1 \overset{\text{def}}{=} z_{(6)} = 2^{-v_2(z)}3^{-v_3(z)}z$ for the coprime to $2\cdot 3$ part of z.

(i) If $z_1 < 19$, then $(\delta_2 x^2, \delta_3 y^3, z^t)$ belongs to one of the following:

$$(3^2, -2^3, 1), (71^2, -17^3, 2^7), (13^2, 7^3, 2^9), (-1549034^2, 15613^3, 33^8), (21063928^2, -76271^3, 17^7).$$

(ii) Suppose that $t \ge 11$ and $z \ge 2$. Then t is not a multiple of $6, 7, 8, 9, 10, 15$, hence t is a multiple of some prime number $q \ge 5$; we have $z_1 \ge 13$, and z_1 is not a power of 5, 7 or 11.

Proof. For assertion (i), write $t_2 \overset{\text{def}}{=} v_2(z)$, $t_3 \overset{\text{def}}{=} v_3(z)$; write r (resp. r_2; r_3) for the residue of t (resp. t_2t; t_3t) modulo 6; let $k \ge 0$ (resp. k_2; k_3) be a integer such that $6k = t - r$ (resp. $6k_2 = t_2t - r_2$; $6k_3 = t_3t - r_3$). Then we have

$$(2^{-3k_2}3^{-3k_3}z_1^{-3k}x)^2 = (-\delta_2\delta_3 2^{-2k_2}3^{-2k_3}z_1^{-2k}y)^3 + \delta_2 2^{r_2}3^{r_3}z_1^r.$$

Hence $P = (-\delta_2\delta_3 2^{-2k_2}3^{-2k_3}z_1^{-2k}y, 2^{-3k_2}3^{-3k_3}z_1^{-3k}x)$ is a rational point on the elliptic curve $Y^2 = X^3 + \delta_2 2^{r_2}z_1^r$, whose denominators of coordinates are divided by z_1, and are divided by 2 (resp. 3) when $r_2 > 0$ (resp. $r_3 > 0$). When $z_1 < 19$, since $\gcd(6, z_1) = 1$, we have $z_1 \in \{1, 5, 7, 11, 13, 17\}$.

When $r > 0$, for $\delta_2 \in \{\pm 1\}$, $z_1 \in \{1, 5, 7\}$, $0 \le r_2, r_3 \le 5$, $1 \le r \le 5$, let S be the set of all prime divisors of $6z_1$. Using Magma [8], we can find all the possible P by computing the S-integral points on the elliptic curve $Y^2 = X^3 + \delta_2 2^{r_2}3^{r_3}z_1^r$, and then choosing the S-integral points whose denominators of coordinates are divided by z_1, and are divided by 2 (resp. 3) when $r_2 > 0$ (resp. $r_3 > 0$). These possible S-integral points imply that $(\delta_2 x^2, \delta_3 y^3, z^t) = (3^2, -2^3, 1)$, $(71^2, -17^3, 2^7)$, $(13^2, 7^3, 2^9)$, $(-1549034^2, 15613^3, 33^8)$, $(21063928^2, -76271^3, 17^7)$. For the Magma codes, cf. [37].

When $r = 0$, we have $6 \mid t$. Then since the only positive coprime solution to $\pm x^2 \pm y^3 = (z^{t/6})^6 = (z')^6$ is the Catalan solution $3^2 - 2^3 = 1^6$, we can deduce that $z^{t/6} = 1$, hence $(\delta_2 x^2, \delta_3 y^3, z^t) = (3^2, -2^3, 1)$. This proves assertion (i).

Since all the solutions in (i) have $z = 1$ or $t < 11$, and the generalized Fermat equation has been solved for the signature $(2, 3, n)$, where $n \in \{6, 7, 8, 9, 10, 15\}$ [cf. Introduction]. Assertion (ii) follows directly from these observations. □

Lemma 3.2. Let $t \ge 11$ be a positive integer, (x, y, z) be a triple of positive coprime integers such that $z \ge 2$ and $\delta_2 x^2 + \delta_3 y^3 = z^t$, where $\delta_2, \delta_3 \in \{\pm 1\}$. Let $l \ge 11$ be a prime number such that $l \ne 13$.

(i) Let $(a, b, c) = (x, \delta_2\delta_3 y, \delta_2 z^t)$, then $a^2 + b^3 = c$, $\gcd(a, b, c) = 1$. Let E be the elliptic curve defined over $\mathbb{Q}$ by the equation

$$Y^2 = X^3 + 3bX + 2a,$$

then the j-invariant

$$j(E) = \frac{1728\delta_3 y^3}{z^t} \notin J \overset{\text{def}}{=} \{0, 2^6 \cdot 3^3, 2^2 \cdot 7^3 \cdot 3^{-4}, 2^{14} \cdot 31^3 \cdot 5^{-3}\}.$$

Write

$$N \overset{\text{def}}{=} z^t / \gcd(1728, z^t),\ N_l \overset{\text{def}}{=} N^{\langle l \rangle},\ N_l' \overset{\text{def}}{=} (N/N_l)_{(l)},\ N_{2l}' \overset{\text{def}}{=} (N/N_l)_{(2l)}.$$

Then $x, y, z \ge 2$, N is the denominator of $j(E)$ and N is not a power of 2.

(ii) Write $F \overset{\text{def}}{=} \mathbb{Q}(E[12])$, then when $N_l' \ne 1$, by the construction in [38], Proposition 2.5, there exists a μ_6-initial Θ-data $\mathfrak{D} = \mathfrak{D}(E, F, l, \mu_6)$ of type (l, N, N_l').

Let $\mathfrak{R}_l^{(1)}$ be the ramification dataset [cf. [38], Definition 1.12] consists of the following data:

$$l_0 = l,\ e_0 = 12,\ S_0 = \{2, 3, l\},\ S_{\text{gen}}^{\text{multi}} = \{e : e \mid 12l\},\ S_2^{\text{good}} = \{e : e \mid 2^8 \cdot 3^2, 2 \mid e\},$$
$$S_3^{\text{good}} = \{e : e \mid 2^6 \cdot 3^2, 2 \mid e\},\ S_l^{\text{good}} = \{l - 1, l(l-1), l^2 - 1\},$$
$$S_2^{\text{multi}} = \{e : e \mid 24l, 2 \mid e\},\ S_3^{\text{multi}} = \{e \mid 48l, 2 \mid e\},\ S_l^{\text{multi}} = \{(l-1) \cdot e : e \mid 12l\}.$$

Then $\mathfrak{D}$ admits $\mathfrak{R}_l^{(1)}$. Hence we have

$$\frac{1}{6}\log(N_l') \le \frac{l^2 + 5l}{l^2 + l - 12} \cdot \Big((1 - \frac{1}{12l}) \cdot \log \operatorname{rad}(N) - \frac{1}{12}(1 - \frac{1}{l}) \log \operatorname{rad}(N_l)\Big) + \operatorname{Vol}(\mathfrak{R}_l^{(1)}). \quad (3.1)$$

The above inequality holds for $N_l' = 1$.

(iii) By Lemma 3.1, we can choose a prime number $q \geq 5$, such that $q \mid t$. Write $F \overset{\text{def}}{=} \mathbb{Q}(\sqrt{-1}, E[2q])$, and suppose that $l \nmid q(q^2-1)$, then when $N'_{2l} \neq 1$, by the construction in Proposition 1.3, there exists a 2-torsion initial Θ-data $\mathfrak{D} = \mathfrak{D}(E, F, l, 2\text{-tor})$ of type (l, N, N'_{2l}).

Let $\mathfrak{R}^{(2)}_{l,q}$ be the ramification dataset [cf. [38], Definition 1.12] consists of the following data:

$$l_0 = l,\ e_0 = 2,\ S_0 = \{2, 3, q, l\},\ S^{\text{multi}}_{\text{gen}} = \{1, 2, l, 2l\},$$
$$S^{\text{good}}_2 = \{e : e \mid 2^5 \cdot 3^2, 2 \mid e\},\ S^{\text{good}}_3 = \{1\},\ S^{\text{good}}_q = \{q-1, q(q-1), q^2-1\},$$
$$S^{\text{good}}_l = \{l-1, l(l-1), l^2-1\},\ S^{\text{multi}}_2 = \{e : e \mid 8ql, 2 \mid e\},\ S^{\text{multi}}_3 = \{e \mid 2ql, 2 \mid e\},$$
$$S^{\text{multi}}_q = \{(q-1)\cdot e : e \mid 2l\},\ S^{\text{multi}}_l = \{(l-1)\cdot e : e \mid 2l\}.$$

Then $\mathfrak{D}$ admits $\mathfrak{R}^{(2)}_{l,q}$. Hence we have

$$\frac{1}{6}\log(N'_{2l}) \leq \frac{l^2+5l}{l^2+l-12} \cdot \big((1-\frac{1}{2l}) \cdot \log \mathrm{rad}(N) - \frac{1}{2}(1-\frac{1}{l}) \log \mathrm{rad}(N_l)\big) + \mathrm{Vol}(\mathfrak{R}^{(2)}_l). \tag{3.2}$$

The above inequality holds for $N'_{2l} = 1$.

Proof. For assertion (i), $j(E) = \frac{1728\delta_3 y^3}{z^t}$ follows from Corollary 1.8, (i). Then since $[z]_2 \geq 13$ by Lemma 3.1, we can see that $j(E) \notin J$, and N is not a power of 2.

For assertion (ii), since $j(E) \notin J$, N is not a power of 2, $N'_l \neq 1$, E_F is semi-stable [cf. Corollary 1.6], $l \geq 11$ and $l \neq 13$, $F = \mathbb{Q}(E[12])$ is Galois over $\mathbb{Q}$ [cf. [38], Proposition 2.1], by the construction in [38], Proposition 2.5, there exists a μ_6-initial Θ-data $\mathfrak{D} = \mathfrak{D}(E, F, l, \mu_6)$ of type (l, N, N'_l). Then by Corollary 1.6, we can see that $\mathfrak{D}$ admits $\mathfrak{R}^{(1)}_l$, hence by Corollary 1.2 we have (3.1). Since the log-volume of a ramification dataset is non-negative, we have $\mathrm{Vol}(\mathfrak{R}^{(1)}_l) \geq 0$, hence (3.1) holds for $N'_l = 1$.

For assertion (iii), by using Corollary 1.8 instead of Corollary 1.6, and using Proposition 1.3 instead of [38], Proposition 2.5, assertion (iii) can be proved similarly to the proof of assertion (ii).

□

Lemma 3.3. Let $t \geq 11$ be a positive integer, (x, y, z) be a triple of positive coprime integers such that $z \geq 2$ and $\delta_2 x^2 + \delta_3 y^3 = z^t$, where $\delta_2, \delta_3 \in \{\pm 1\}$.

Let S be a finite set of prime numbers with cardinality $n = |S| \geq 2$, such that for each $l \in S$, we have $l \geq 11$, $l \neq 13$; let $2 \leq k \leq S$ be a positive integer, p_0 be the smallest prime number in S, $k(S)$ be the product of k smallest prime numbers in S; let $n_0 = \gcd(1728, z^t)$, $N = n_0^{-1} z^t$;

for each $l \in S$, write $\mathrm{Vol}(l) \overset{\text{def}}{=} \mathrm{Vol}(\mathfrak{R}^{(1)}_l)$ [cf. Lemma 3.2]; let $e_0 = 12$, $S_1 = \{2, 3\}$, $p_B = 2$, $n_k(S)$ be the product of the smallest k prime numbers in S.

Let S be a finite set of prime numbers with cardinality $n = |S| \geq 2$, such that for each $l \in S$, we have $l \geq 11$; let $2 \leq k \leq S$ be a positive integer, p_0 be the smallest prime number in S, $k(S)$ be the product of k smallest prime numbers in S; let $n_0 = 2^8$, $N = n_0^{-1} x^{2r} y^{2s} z^{2t}$, $u_0 = 8$, $p_N = 2$, $e_0 = 3$, $S_1 = \{2\}$, $n_1(S) = 2p_0$, $n_k(S) = 2k(S)$; for each $l \in S$, write $\mathrm{Vol}(l) \overset{\text{def}}{=} \mathrm{Vol}(\mathfrak{R}^{(1)}_l)$, cf. Lemma 2.1, (ii). Suppose that one of the following situations is satisfied:

(i) Let $u_0 \geq 11$ be a positive integer, such that $u_0 \leq t$; let $n_1(S) = u_0$.

(ii) Suppose that for each $l \in S$, we have $l \nmid t$. Let $u_0 = t$, $n_1(S) = p_0 t$.

Then with the notation in (i) or (ii), the assumptions in Definition 1.11 are satisfied, and we can define b_1, b_2. Note that with the notation in (i), the definitions of b_1, b_2 are independent to $t \geq u_0$. Hence if we have $b_1 < 1$ and $n_k(S) \cdot \log(2) > \frac{b_2}{1-b_1}$, then by Lemma 1.12, $\log(N)$ cannot belong to the interval $(\frac{b_2}{1-b_1}, n_k(S) \cdot \log(2))$.

Proof. The proof follows from Lemma 3.2 and is elementary, which is similar to the proof of Lemma 2.2. □

Lemma 3.4. Let $t \geq 11$ be a positive integer, (x, y, z) be a triple of positive coprime integers such that $z \geq 2$ and $\delta_2 x^2 + \delta_3 y^3 = z^t$, where $\delta_2, \delta_3 \in \{\pm 1\}$.

Let q be a prime number ≥ 5, such that $q \mid t$. Let S be a finite set of prime numbers with cardinality $n = |S| \geq 2$, such that for each $l \in S$, we have $l \geq 11$, $l \neq 13$ and $l \nmid q(q^2 - 1)$. let p_0 be the smallest prime number in S; $2 \leq k \leq S$ be a positive integer; $n_0 = \gcd(27, z^t)$, $N \stackrel{\text{def}}{=} n_0^{-1}[z^t]_2$, $e_0 = 2$; for each $l \in S$, write $\mathrm{Vol}(l) \stackrel{\text{def}}{=} \mathrm{Vol}(\mathfrak{R}_l^{(2)}) + \log(2)$ [cf. Lemma 3.2].

Let $u_0 = t$, $S_1 = \{3\}$, $n_1(S) = t$, $p_B = 3$, $n_k(S)$ be the product of the smallest k prime numbers in S. Then the assumptions in Definition 1.11 are satisfied, and we can define b_1, b_2. Hence if we have $b_1 < 1$ and $n_k(S) \cdot \log(3) > \frac{b_2}{1-b_1}$, then by Lemma 1.12, $\log(N)$ cannot belong to the interval $(\frac{b_2}{1-b_1}, n_k(S) \cdot \log(3))$.

Proof. Since $\log \mathrm{rad}(N) \leq \log \mathrm{rad}([N]_2) + \log(2)$, the proof follows from Lemma 3.3 and is elementary, which is similar to the proof of Lemma 2.2. □

Proposition 3.5. Let $t \geq 11$ be a positive integer, (x, y, z) be a triple of positive coprime integers such that $z \geq 2$ and $\delta_2 x^2 + \delta_3 y^3 = z^t$, where $\delta_2, \delta_3 \in \{\pm 1\}$. Write $z_1 \stackrel{\text{def}}{=} 2^{-v_2(z)} z$ for the coprime to 2 part of z.

(i) We have $z_1 \geq 13$; the exponent t is not divided by $6, 7, 8, 9, 10, 15$, hence We have $t \in \{11, 13\}$ or $17 \leq t < 1000$.

(ii) We have $\log(z^t) < 3730$ for $t = 11$; $\log(z^t) < 3085$ for $t = 13$; and $\log(z^t) < 2789$ for $t \geq 17$.

(iii) We have $t \leq 353$ or $t = 373$. In addition, we have $\log(z_1^t) < 1183$ for $t = 11$; $\log(z_1^t) < 994$ for $t = 13$; $\log(z_1^t) < 919$ for $t = 17$; $\log(z_1^t) < 895$ for $t = 19$; $\log(z_1^t) < 1019$ for $t = 373$; and $\log(z_1^t) < 981$ for $t \geq 17$, $t \neq 373$.

Proof. For assertion (i), by Lemma 3.1, we have $z_1 \geq 13$; the exponent t is not divided by $6, 7, 8, 9, 10, 15$, hence $t \in \{11, 13\}$ or $t \geq 17$. Then by Lemma 3.3, (i) and the computation in [37], we have $\log(z^t) < 2560$ for $t \geq 1000$. But since $z \geq z_1 \geq 13$, if $t \geq 1000$, then $\log(z^t) \geq 1000 \cdot \log(13) > 2564$ — a contradiction! Hence $t < 1000$.

assertion (ii) follows from Lemma 3.3, (ii) and the computation in [37]. assertion (iii) follows from Lemma 3.4 and the computation in [37]. □

Corollary 3.6. For any integer $n \geq 3$, there does not exist any triple (x, y, z) of non-zero coprime integers that satisfies the generalized Fermat equation

$$x^2 + y^{2n} = z^3.$$

Proof. Suppose that for some $n \geq 3$, there exists a triple of non-zero coprime integers (x, y, z) such that $x^2 + y^{2n} = z^3$. Then we have $n > 10^7$, cf. Chen [13], Dahmen [16]. Hence by Proposition 3.5, we have $|y| = 1$, $x^2 + 1 = y^3$. However, the only integral points on the elliptic curve $Y^2 = X^3 - 1$ are $(1, 0)$ and the point at infinity. Hence $(x, y) = (0, 1)$, which is impossible! Hence the generalized Fermat equation $x^2 + y^{2n} = z^3$ has no non-trivial primitive solution. □

3.2 Structure of solutions

We shall analyze the structure of the solution (x, y, z) in more detail.

Lemma 3.7. Let $t \geq 60$ be a positive integer, (x, y, z) be a triple of positive coprime integers such that $z \geq 2$ and $\delta_2 x^2 + \delta_3 y^3 = z^t$, where $\delta_2, \delta_3 \in \{\pm 1\}$. Let $q \geq 5$ be a prime number, such that $q \mid t$.

Let S be the set of prime numbers $p \geq 11$, such that $p \neq 13$, $p \nmid t$ and $p \nmid (q^2 - 1)$. For each $p \in S$, denote [cf. Lemma 4.1]

$$a_1(p) \stackrel{\text{def}}{=} 6 \cdot \frac{p^2 + 5p}{p^2 + p - 12} \cdot (1 - \frac{1}{2p}),\ a_2(p) \stackrel{\text{def}}{=} 6 \cdot \mathrm{Vol}(\mathfrak{R}_{l,q}^{(2)}) + a_1(p) \cdot \log(6p).$$

Let $l \in S$, write uniquely

$$z = z_1 \cdot 2^{t_2} \cdot 3^{t_3} \cdot l^{t_l} \cdot z_l^l, \tag{3.3}$$

where $z_1, z_l, 2, 3, l$ are pairwise coprime positive integers, $t_2, t_3, t_l \geq 0$, $z_l^l = z_{(6l)}^{\langle l \rangle}$.

(i) We have $z_l = 1$, hence

$$a_2(l) \geq t \cdot \log(z_1) - a_1(l) \cdot \log \mathrm{rad}(z_1) \geq (t - a_1(l)) \cdot \log(z_1). \tag{3.4}$$

(ii) Let p be a prime divisor of z. When $t \geq 93$, we have $p \leq 31$; when $t \geq 110$ and $t \neq 113, 121$, we have $p \leq 17$.

(iii) When $t \geq 95$, we have $z_{(6)} < 43$; when $t \geq 107$, we have $z_{(6)} < 35$.

(iv) We have $t \leq 109$ or $t = 113, 121$.

Proof. For assertion (i), by Proposition 3.5, we have $1019 > \log(z_{(2)}^t) \geq z_l^{tl}$, hence $\log(z_l) < \frac{1019}{tl} \leq \frac{1019}{60 \cdot 11} < \log(5)$, $z_l < 5$. Then since $\gcd(6l, z_l) = 1$, we have $z_l = 1$. Hence $\log(z_1^t) \leq \log(N'_{2l})$, $\log \mathrm{rad}(N) \leq \log \mathrm{rad}(6lz_1)$, and (3.4) follows from (3.2).

For assertion (ii), choose $l \in S$ such that $l \neq p$, then we have $p \mid z_1$. Hence by (3.4), we have $\log(p) \leq \log(z_1) \leq \frac{a_2(l)}{t - a_1(l)}$. Recall that $t < 400$ [cf. Proposition 3.5, (iii)]. For each $95 \leq t < 400$, we can choose such l explicitly, and get upper bounds for each possible p. Then assertion (ii) follows from the computation in [37].

For assertion (iii), we can choose $l \in S$ such that $l \nmid z_1$ explicitly, then by (3.4), we have $\log(z_1) \leq \frac{a_2(l)}{t - a_1(l)}$. Then assertion (ii) follows from the computation in [37].

For assertion (iv), assume that $t \geq 110$ and $t \neq 113, 121$, then by (ii), $z_{(6)}$ only has prime divisors $\in \{5, 7, 11, 13, 17\}$. Then since by (iii) we have $z_{(6)} < 35$, hence $z_{(6)} \in \{1, 5, 7, 11, 13, 17, 25\}$. But this contradicts Lemma 3.1, (ii), hence assertion (iv) holds. □

Corollary 3.8. Suppose that (r, s, t) is a permutation of $(2, 3, n)$ with $n \geq 7$, such that n does not satisfy the following conditions:

- $11 \leq n \leq 109$ or $n \in \{113, 121\}$.
- n is not divided by $6, 7, 8, 9, 10, 15$.

Then the generalized Fermat equation $x^r + y^s = z^t$ has no non-trivial primitive solution except for the solutions related to the Catalan solutions and the nine non-Catalan solutions enumerated in the introduction.

Proof. Suppose that (x, y, z) is a non-trivial primitive solution to the equation $x^r + y^s = z^t$, such that $|x|, |y|, |z| \geq 2$. By interchanging (r, s, t), we can assume without loss of generality that $(r, s, t) = (2, 3, n)$, and (x, y, z) is a triple of positive coprime integers such that $z \geq 2$ and $\delta_2 x^2 + \delta_3 y^3 = z^t$, where $\delta_2, \delta_3 \in \{\pm 1\}$.

Since the signatures $(2, 3, n)$ with $n \in \{6, 7, 8, 9, 10, 15\}$ have been solved [cf. Introduction], we have $n \geq 11$ and n is not divided by $6, 7, 8, 9, 10, 15$. Then by Lemma 3.7, we have $n \leq 109$ or $n \in \{113, 121\}$. □

4 The signatures $(3, r, s)$

Let $r, s \geq 3$ be positive integers. In this section, we shall consider about the generalized Fermat equation with signature $(3, r, s)$ or its permutation. Since the signatures $(3, 3, n)$ and its permutations have been solved for $n \geq 3$ [cf. [38]], and the signatures $(3, 4, 5), (3, 5, 5)$ and their permutations have been solved [cf. Introduction], we only need to consider for $r, s \geq 4$, $\max\{r, s\} \geq 7$ and $3 \nmid rs$.

4.1 Upper bounds

In this section, we shall assume that $r, s \geq 4$ are positive integers, (x, y, z) is a triple of positive coprime integers such that $\delta_r x^r + \delta_s y^s = z^3$, where $\delta_r, \delta_s \in \{\pm 1\}$.

Lemma 4.1. Let $r, s \geq 4$ be positive integers, (x, y, z) be a triple of positive coprime integers such that $\delta_r x^r + \delta_s y^s = z^3$, where $\delta_r, \delta_s \in \{\pm 1\}$. Let $l \geq 11$ be a prime number such that $l \neq 13$.

(i) Let $(a, b, c) = (\delta_r x^r, \delta_s y^s, z)$, then $a + b = c^3$, $\gcd(a, b, c) = 1$. Let E be the elliptic curve defined over $\mathbb{Q}$ by the equation

$$Y^2 + 3cXY + aY = X^3,$$

then E is an elliptic curve with

$$j(E) = \frac{27c^3(a + 9b)^3}{a^3 b} = \frac{27c^3(a + 9b)^3}{\delta_r \delta_s x^{3r} y^s} \notin J \overset{\text{def}}{=} \{0, 2^6 \cdot 3^3, 2^2 \cdot 73^3 \cdot 3^{-4}, 2^{14} \cdot 31^3 \cdot 5^{-3}\}.$$

Write

$$N \overset{\text{def}}{=} x^{3r} y^s / \gcd(27, x^{3r} y^s),\ N_l \overset{\text{def}}{=} N^{\langle l \rangle},\ N_l' \overset{\text{def}}{=} (N/N_l)_{(l)},\ N_{2l}' \overset{\text{def}}{=} (N/N_l)_{(2l)}.$$

Then $x, y, z \geq 2$, N is the denominator of $j(E)$ and N is not a power of 2.

(ii) Write $F \overset{\text{def}}{=} \mathbb{Q}(E[12])$, then when $N_l' \neq 1$, by the construction in [38], Proposition 2.5, there exists a μ_6-initial Θ-data $\mathfrak{D} = \mathfrak{D}(E, F, l, \mu_6)$ of type (l, N, N_l').

Let $\mathfrak{R}_l^{(1)}$ be the ramification dataset [cf. [38], Definition 1.12] consists of the following data:

$$l_0 = l,\ e_0 = 12,\ S_0 = \{2, 3, l\},\ S_{\text{gen}}^{\text{multi}} = \{e : e \mid 12l\},\ S_2^{\text{good}} = \{e : e \mid 2^8 \cdot 3^2, 2 \mid e\},$$
$$S_3^{\text{good}} = \{e : e \mid 2^6 \cdot 3^2, 2 \mid e\},\ S_l^{\text{good}} = \{l - 1, l(l - 1), l^2 - 1\},$$
$$S_2^{\text{multi}} = \{e : e \mid 24l, 2 \mid e\},\ S_3^{\text{multi}} = \{e \mid 48l, 2 \mid e\},\ S_l^{\text{multi}} = \{(l - 1) \cdot e : e \mid 12l\}.$$

Then $\mathfrak{D}$ admits $\mathfrak{R}_l^{(1)}$. Hence we have

$$\frac{1}{6} \log(N_l') \leq \frac{l^2 + 5l}{l^2 + l - 12} \cdot \big((1 - \frac{1}{12l}) \cdot \log \operatorname{rad}(N) - \frac{1}{12}(1 - \frac{1}{l}) \log \operatorname{rad}(N_l)\big) + \operatorname{Vol}(\mathfrak{R}_l^{(1)}). \quad (4.1)$$

The above inequality holds for $N_l' = 1$.

(iii) Write $F \overset{\text{def}}{=} \mathbb{Q}(E[4])$, then when $N_{2l}' \neq 1$, by the construction in Proposition 1.3, there exists a 2-torsion initial Θ-data $\mathfrak{D} = \mathfrak{D}(E, F, l, 2\text{-tor})$ of type (l, N, N_{2l}').

Let $\mathfrak{R}_l^{(2)}$ be the ramification dataset [cf. [38], Definition 1.12] consists of the following data:

$$l_0 = l,\ e_0 = 4,\ S_0 = \{2, 3, l\},\ S_{\text{gen}}^{\text{multi}} = \{e : e \mid 4l\},\ S_2^{\text{good}} = \{e : e \mid 96, 2 \mid e\},$$
$$S_3^{\text{good}} = \{e : e \mid 12, 2 \mid e\},\ S_l^{\text{good}} = \{l-1, l(l-1), l^2-1\},$$
$$S_2^{\text{multi}} = \{e : e \mid 8l, 2 \mid e\},\ S_3^{\text{multi}} = \{e \mid 8l, 2 \mid e\},\ S_l^{\text{multi}} = \{(l-1)\cdot e : e \mid 4l\}.$$

Let $\mathfrak{R}_l^{(3)}$ be the ramification dataset obtained by setting $S_l^{\text{good}} = \emptyset$ in the definition of $\mathfrak{R}_l^{(2)}$. Then $\mathfrak{D}$ admits $\mathfrak{R}_l^{(3)}$; and if $l \mid xy$, then $\mathfrak{D}$ admits $\mathfrak{R}_l^{(3)}$. Hence we have

$$\frac{1}{6}\log(N_{2l}') \leq \frac{l^2+5l}{l^2+l-12} \cdot \big((1-\frac{1}{4l})\cdot \log \mathrm{rad}(N) - \frac{1}{4}(1-\frac{1}{l})\log \mathrm{rad}(N_l)\big) + \mathrm{Vol}(l). \tag{4.2}$$

where we write $\mathrm{Vol}(l) \overset{\text{def}}{=} \mathrm{Vol}(\mathfrak{R}_l^{(2)})$ if $l \nmid xyz$, and write $\mathrm{Vol}(l) \overset{\text{def}}{=} \mathrm{Vol}(\mathfrak{R}_l^{(3)}) \leq \mathrm{Vol}(\mathfrak{R}_l^{(2)})$ if $l \mid xyz$. The above inequality holds for $N_{2l}' = 1$.

Proof. For assertion (i), $j(E) = \frac{27c^3(a+9b)^3}{a^3b}$ follows from Corollary 1.9, (i). Then since $r, s \geq 5$, by Catalan's conjecture we have $x, y, z \geq 2$. Hence we can see that $j(E) \notin J$, and N is not a power of 2.

The proof of assertions (ii) and (iii) are similar to that of Lemma 2.1. □

Lemma 4.2. Let $r \geq 4$, $s \geq 7$ be positive integers, (x, y, z) be a triple of positive coprime integers such that $\delta_r x^r + \delta_s y^s = z^3$, where $\delta_r, \delta_s \in \{\pm 1\}$.

Let S be a finite set of prime numbers with cardinality $n = |S| \geq 2$, such that for each $l \in S$, we have $l \geq 11$, $l \neq 13$; let $2 \leq k \leq S$ be a positive integer, p_0 be the smallest prime number in S, $k(S)$ be the product of k smallest prime numbers in S; let $n_0 = \gcd(27, x^{3r}y^s)$, $N \overset{\text{def}}{=} n_0^{-1}x^{3r}y^s$, $7 \leq u_0 \leq \min\{3r, s\}$, $p_N = 2$, $e_0 = 12$, $S_1 = \{3\}$, $n_1(S) = p_0$, $n_k(S) = k(s)$; for each $l \in S$, write $\mathrm{Vol}(l) \overset{\text{def}}{=} \mathrm{Vol}(\mathfrak{R}_l^{(1)})$, cf. Lemma 4.1. Suppose that one of the following situations is satisfied:

(a) Let $u_0' \geq u_0$ be a positive integer, $P \subseteq \{p : v_p(N) \geq u_0'\} \cup \{p : p \nmid N\}$, $n_1'(S) = \max\{u_0', 2p_0\}$. In particular, we can let $u_0' = \min\{3r, s\}$, $P = \{p : p \mid N\}$, $n_0' = n_0$ and $N' = N$.

(b) Let $u_0' \geq u_0$ be a positive integer, $P \subseteq \{p : v_p(N) \geq u_0'\} \cup \{p : p \nmid N\}$, $n_1'(S) = \min\{v_p(N) : p \in B' \setminus S_1\}$ [for the definition of B', cf. Definition 1.5, (e)], $n_0' = 27$ if $3 \in P$ and $n_0' = 1$ if $2 \notin P$.

(c) In the situation of (b). if $l \nmid rs$ for each $l \in S$, then we can let $u_0' = \min\{3r, s\}$, $n_1'(S) = u_0'p_0$, $P = \{p : p \mid xy\}$, $N' = (n_0')^{-1}x^{3r}y^s$; if $l \nmid r$ for each $l \in S$, then we can let $u_0' = 2r$, $n_1'(S) = u_0'p_0$, $P = \{p : p \mid x\}$, $N' = (n_0')^{-1}x^{3r}$; if $l \nmid s$ for each $l \in S$, then we can let $u_0' = s$, $n_1'(S) = u_0'p_0$, $P = \{p : p \mid y\}$, $N' = (n_0')^{-1}y^s$.

Then the assumptions in Definition 1.11 are satisfied, and we can define b_1, b_2, b_1'. Hence if $b_1 \leq 1$, $b_1' < 1$ and $n_k(S)\cdot\log(2) > \frac{b_2}{1-b_1'}$, then by Lemma 1.12, $\log(N')$ cannot belong to the interval $(\frac{b_2}{1-b_1'}, n_k(S)\cdot\log(2))$.

Proof. The proof follows from Lemma 4.1 and is elementary, which is similar to the proof of Lemma 2.2. □

Lemma 4.3. Let $r \geq 4$, $s \geq 7$ be positive integers, (x, y, z) be a triple of positive coprime integers such that $\delta_r x^r + \delta_s y^s = z^3$, where $\delta_r, \delta_s \in \{\pm 1\}$.

Let S be a finite set of prime numbers with cardinality $n = |S| \geq 2$, such that for each $l \in S$, we have $l \geq 11$, $l \neq 13$; let $2 \leq k \leq S$ be a positive integer, p_0 be the smallest prime number in S, $k(S)$ be the product of k smallest prime numbers in S; let $n_0 = \gcd(27, x^{3r}y^s)$, $N \overset{\text{def}}{=} (n_0^{-1}x^{3r}y^s)_{(2)}$, $7 \leq u_0 \leq \min\{3r, s\}$, $p_N = 3$, $e_0 = 4$, $S_1 = \{3\}$, $n_1(S) = p_0$, $n_k(S) = k(s)$; for each $l \in S$, write $\mathrm{Vol}(l) \overset{\text{def}}{=} \mathrm{Vol}(\mathfrak{R}_l^{(2)}) + \log(2)$, cf. Lemma 4.1. Suppose that one of the following situations is satisfied:

(a) Let $u_0' \geq u_0$ be a positive integer, $P \subseteq \{p : v_p(N) \geq u_0'\} \cup \{p : p \nmid N\}$, $n_1'(S) = \max\{u_0', 2p_0\}$. In particular, we can let $u_0' = \min\{3r, s\}$, $P = \{p : p \mid N\}$, $n_0' = n_0$ and $N' = N$.

(b) Let $u_0' \geq u_0$ be a positive integer, $P \subseteq \{p : v_p(N) \geq u_0'\} \cup \{p : p \nmid N\}$, $n_1'(S) = \min\{v_p(N) : p \in B' \setminus S_1\}$ [for the definition of B', cf. Definition 1.5, (e)], $n_0' = 27$ if $3 \in P$ and $n_0' = 1$ if $2 \notin P$.

(c) In the situation of (b). if $l \nmid rs$ for each $l \in S$, then we can let $u_0' = \min\{3r, s\}$, $n_1'(S) = u_0'p_0$, $P = \{p : p \mid xy\}$, $N' = (n_0')^{-1}x^{3r}y^s$; if $l \nmid r$ for each $l \in S$, then we can let $u_0' = 2r$, $n_1'(S) = u_0'p_0$, $P = \{p : p \mid x\}$, $N' = (n_0')^{-1}x^{3r}$; if $l \nmid s$ for each $l \in S$, then we can let $u_0' = s$, $n_1'(S) = u_0'p_0$, $P = \{p : p \mid y\}$, $N' = (n_0')^{-1}y^s$.

Then the assumptions in Definition 1.11 are satisfied, and we can define b_1, b_2, b_1'. Hence if $b_1 \leq 1$, $b_1' < 1$ and $n_k(S) \cdot \log(2) > \frac{b_2}{1-b_1'}$, then by Lemma 1.12, $\log(N')$ cannot belong to the interval $(\frac{b_2}{1-b_1'}, n_k(S) \cdot \log(3))$.

Proof. The proof follows from Lemma 4.1 and is elementary, which is similar to the proof of Lemma 2.2. □

Proposition 4.4. Let $r, s \geq 4$ be positive integers, (x, y, z) be a triple of positive coprime integers such that $\delta_r x^r + \delta_s y^s = z^3$, where $\delta_r, \delta_s \in \{\pm 1\}$.

(i) We have $x, y, z \geq 2$, $\max\{r, s\} \geq 7$ and $3 \nmid rs$; when $r \in \{4, 5\}$, we have $7 \leq s \leq 3677$; when $r \geq 4$, $s \geq 7$, we have $\log(x^{3r}y^s) < 31000$.

(ii) Suppose that $r, s \geq 7$, Then we have $7 \leq r, s \leq 1226$, $\log(x^r), \log(y^s) \leq 1400$,

(iii) Suppose that $r \geq 7$, $s \geq 21$. Let $x_{(2)}, y_{(2)}$ be the coprime to 2 part of x and y respectively. Then we have $\log(x_{(2)}^{3r}y_{(2)}^s) \leq 1481$, $\log(y_{(2)}^{3s}x_{(2)}^r) \leq 1207$, $\log(x_{(2)}^r) \leq 494$ and $\log(y_{(2)}^s) \leq 403$.

Proof. The proposition follows from Lemma 4.2, Lemma 4.3 and the computation in [37]. □

4.2 Structure of solutions

We shall analyze the structure of the solution (x, y, z) in more detail.

Lemma 4.5. Let $r \geq 7$, $s \geq 8$ be positive integers, (x, y, z) be a triple of positive coprime integers such that $\delta_r x^r + \delta_s y^s = z^3$, where $\delta_r, \delta_s \in \{\pm 1\}$.

For each prime number $p \geq 17$, denote [cf. Lemma 4.1]

$$a_1(p) \overset{\text{def}}{=} 6 \cdot \frac{p^2+5p}{p^2+p-12} \cdot (1 - \frac{1}{4p}),$$
$$a_2(p) \overset{\text{def}}{=} 6 \cdot \mathrm{Vol}(\mathfrak{R}_p^{(2)}) + a_1(p) \cdot \log(6), 3 \cdot \mathrm{Vol}(\mathfrak{R}_p^{(3)}) + a_1(p) \cdot \log(6p)\}.$$

Then we have $6 < a_1(p) < 7.6$, and we have $a_2(17) < 403$, $a_2(19) < 425$, $a_2(23) < 472$, $a_2(29) < 544$, $a_2(31) < 578$.

Let $l \geq 17$ be a prime number such that $l \nmid rs$. Write uniquely

$$x = x_1 \cdot 2^{r_2} \cdot 3^{r_3} \cdot l^{r_l} \cdot x_l^l, \ y = y_1 \cdot 2^{s_2} \cdot 3^{s_3} \cdot l^{s_l} \cdot y_l^l, \tag{4.3}$$

where $x_1, y_1, x_l, y_l, 2, 3, l$ are pairwise coprime positive integers, $r_2, s_2, r_3, s_3, r_l, s_l \geq 0$, $x_l^l = x_{(6l)}^{\langle l \rangle}$, $y_l^l = y_{(6l)}^{\langle l \rangle}$.

(i) We have $3 \nmid rs$. If $r = 7$, then $s \geq 11$. Moreover, we have

$$\begin{aligned} 3r \cdot \log(x_1) + s \cdot \log(y_1) &\leq a_2(l) + a_1(l) \cdot \log \mathrm{rad}(x_1 y_1 x_l y_l), \\ r \cdot \log(x_1) + 3s \cdot \log(y_1) &\leq a_2(l) + a_1(l) \cdot \log \mathrm{rad}(x_1 y_1 x_l y_l). \end{aligned} \tag{4.4}$$

Hence

$$\begin{aligned} (3r - 7.6) \cdot \log(x_1) \leq 3r \cdot \log(x_1) - a_1(l) \cdot \log \mathrm{rad}(x_1) \leq a_2(l) + a_1(l) \log(x_l y_l), \\ (\frac{20s}{7} - 7.6) \cdot \log(y_1) \leq \frac{20s}{7} \cdot \log(y_1) - a_1(l) \cdot \log \mathrm{rad}(y_1) \leq a_2(l) + a_1(l) \log(x_l y_l). \end{aligned} \tag{4.5}$$

(ii) We have $x_l = 1$, $y_l = 1$, hence we have $a_1(l) \cdot \log(x_l y_l) = 0$ in (4.5).

(iii) Let $p \geq 5$, $p \neq l$ be a prime number. If $l \nmid v_p(x)$, then we have $(3r \cdot v_p(x) - a_1(l)) \cdot \log(p) < a_2(l)$; if $l \nmid v_p(y)$, then we have $(\frac{20}{7} \cdot s \cdot v_p(x) - a_1(l)) \cdot \log(p) < a_2(l)$; if $3 \mid x$ and $l \nmid (3r_3 r - 3)$, then we have $(3r_3 r - 3 - a_1(l)) \cdot \log(3) < a_2(l)$; if $3 \mid y$, $l \nmid (s_3 s - 3)$ and $l \nmid (3s_3 s - 1)$, then we have $(\frac{20}{7} s_3 s - 3 - a_1(l)) \cdot \log(3) < a_2(l)$.

(iv) We have $r_l \leq \frac{56}{r}$, $s_l \leq \frac{56}{s}$.

(v) We have $r_3 \leq \frac{153}{r}$, and $r_3 = 0$ when $r > 137$; $s_3 \leq \frac{153}{s}$, and $s_3 = 0$ when $s > 137$.

Proof. For assertion (i), since all the signatures $(3, 3, n)$for $n \geq 3$, $(3, m, n)$ for $7 \leq m, n \leq 10$ and their permutations have been solved [cf. Introduction], we can deduce that $s \geq 11$, $3 \nmid rs$. Since $l \nmid rs$, following the notation of Lemma 4.1, we have $x_1^{3r} y_1^s \mid N_l'$, $\log \mathrm{rad}(N) \leq \log \mathrm{rad}(x_1 y_1 x_l y_l) + \log(6)$ when $l \nmid xy$, and $\log \mathrm{rad}(N) \leq \log \mathrm{rad}(x_1 y_1 x_l y_l) + \log(6l)$ when $l \mid xy$. Hence the first inequality in (4.4) follows from (4.2). Then since $s > 8 > a_1(l)$, we have $s \cdot \log(y_1) \geq a_1(l) \cdot \log(y_1)$, hence $a_2(l) + a_1(l) \log(x_l y_l) \geq 3r \cdot \log(x_1) - a_1(l) \cdot \log \mathrm{rad}(x_1) \geq (3r - 7.6) \cdot \log(x_1)$.

By symmetry, if we "interchange" (x, r) and (y, s) in Lemma 4.1, then the second inequality in (4.4) follows from (4.2). If $r \geq 8$, then the second inequality in (4.5) can be proved by symmety. Suppose that $r = 7$, then by computing $\frac{1}{14} \times$ "the first line of (4.4)" + $\frac{13}{14} \times$ "the second line of (4.4)", we have

$$8 \cdot \log(x_1) + \frac{20s}{7} \cdot \log(y_1) \leq a_2(l) + a_1(l) \cdot \log \mathrm{rad}(x_1 y_1 x_l y_l).$$

Then assertion (i) follows.

For assertion (ii), recall that we have $\log(x_1 3^{r_3} l^{r_l} x_l^l) = \log(x_{(2)}) \leq \frac{494}{r}$, hence $x_l \leq \exp(\frac{494}{rl}) \leq \exp(\frac{494}{7 \cdot 17}) < 64$. Since $2, 3 \nmid x_l$, we have $x_l \leq 61$. By symmetry, we can prove that $y_l \leq 61$, and note that this is ture for any prime number $l \geq 17$.

When $r \geq 11$, we have $\log(x_l) \leq \frac{494}{100l} < \log(3)$, hence $x_l = 1$. Now suppose that $r < 100$, and by replcaing s by its prime divisor ≥ 11, we can assume that s is divided by at most one prime number ≥ 11.

Let q be the smallest prime number $q \geq 17$, such that $q \neq l$, $q \nmid rs$ and $q \nmid x_l$. Then by the above analysis, at most four prime numbers $p \geq 17$ are excluded, hence we have $q \leq 31$, $a_2(q) < 578$. Write uniquely $x = x_1' \cdot 2^{r_2} \cdot 3^{r_3} \cdot q^{r_q} \cdot x_q^q$, $y = y_1' \cdot 2^{s_2} \cdot 3^{s_3} \cdot q^{s_q} \cdot y_q^q$ similar to (4.3), where $x_1', y_1', x_q, y_q, 2, 3, q$ are pairwise coprime, $r_2, s_2, r_3, s_3, r_q, s_q \geq 0$, $x_q^q = x_{(6q)}^{\langle q \rangle}$, $y_q^q = y_{(6q)}^{\langle q \rangle}$. Since we have $x_q, y_q \leq 61$ [by replacing x_l, y_l by x_q, y_q], then by (4.5) we have $(3r - 7.6) \cdot \log \operatorname{rad}(x_1') \leq a_2(q) + 7.6 \cdot \log(61^2) < a_2(q) + 63 < 641$.

Note that we have $\gcd(x_l, 6q) = 1$, and we claim that $\gcd(x_l, x_q) = 1$. In fact, suppose that we have $p \mid x_l$, $p \mid x_q$ for some prime p, then $p \geq 5$ [since $2, 3 \nmid x_l$] and $ql \mid v_p(x)$ by definition. Hence by Proposition 4.4, we have $494 > \log(x_{(2)}^2) \geq r \cdot v_p(x) \cdot \log(p) \geq rql \cdot \log(5) > 7 \cdot 11 \cdot 17 \cdot \log(5) > 494$ — a contradiction! Hence we have $\gcd(x_l, x_q) = 1$.

Since $x_l^l \mid x = x_1' \cdot 2^{r_2} \cdot 3^{r_3} \cdot q^{r_q} \cdot x_q^q$ and $\gcd(x_l, 6qx_q) = 1$, we can deduce that $x_l^l \mid x_1'$. Then by (i), $641 > a_2(q) + a_1(q) \cdot \log(x_q y_q) \geq 3r \cdot \log(x_1') - 4 \log \operatorname{rad}(x_1') \geq (3rl - 7.6) \log(x_l)$, thus

$$\log(x_l) \leq \frac{a_2(q) + a_1(q) \cdot \log(x_q y_q)}{3rl - 7.6} < \frac{641}{3rl - 7.6}. \tag{4.6}$$

Hence when $r \geq 8$, we have $\log(x_l) \leq \frac{641}{3 \cdot 8 \cdot 17 - 7.6} < \log(5)$, hence $x_l = 1$; then by the symmetry of r, s [since both of them ≥ 8, we can interchange (x, r) and (y, s), we shall use the word "symmetry" to represent this observasion], we have $y_l = 1$.

Now assume that $r = 7$, then $s \geq 11$. We can similar prove that $x_l = 1$ when $l \geq 23$; $x_l \in \{1, 5\}$ when $l \in \{17, 19\}$. Since $s \geq 11$, we can also prove similarly that

$$\log(y_l) \leq \frac{641}{\frac{20s}{7} \cdot l - 7.6} \leq \frac{641}{\frac{20 \cdot 11}{7} \cdot 17 - 7.6} < \log(4),$$

Hence $y_l = 1$. Moreover, when $r = 7$, $x_l \leq 5$, we further have $q \leq 23$, $a_2(q) < 472$. Hence by (4.6) we have $\log(x_l) < \frac{472 + 7.6 \cdot \log(5)}{3 \cdot 7 \cdot 17 - 7.6} < \log(4)$, hence $x_l = 1$. This proves assertion (ii).

Aassertion (iii) is a direct consequence of Lemma 4.1). The proof of assertion (iii) is similar to that of assertion (i).

For assertion (iv), let q be the smallest prime number $q \geq 17$, such that $q \neq l$, $q \nmid rs$ and $q \nmid r_l$. Write uniquely $x = x_1' \cdot 2^{r_2} \cdot 3^{r_3} \cdot q^{r_q}$ similar to (4.3), where $2, 3, q \nmid x_1'$, $r_2, r_3, r_q \geq 0$ [recall that we have proven $x_q = y_q = 1$ in assertion (ii)]. Then by assertion (iii), we have $(3rr_l - a_1(q)) \cdot \log(l) \leq a_2(q)$, thus

$$r_l \leq \frac{a_2(q)/\log(l) + a_1(q)}{3r}. \tag{4.7}$$

One can easily show that $r_l < 100$ at first. Then similar to the proof of assertion (ii), in the choice of q, we can replace r, s by their prime divisors ≥ 17, to exclude at most 4 prime numbers $p \geq 17$, such that $p \mid lrsr_l$. Hence $q \leq 31$, $a_1(q) < 578$, $r_l \leq \frac{578/\log(17) + 7.6}{3 \cdot 7} < 11$, $r_l \leq 10$. Then we have $q \leq 29$, hence

$$r_l r \leq \max_{q \in \{17, 19, 23, 29\}} \frac{a_2(q)/\log(q) + 7.6}{3} < 57,$$

thus $r_l \leq \frac{56}{r}$.

For the upper bound of s_l, when $r \geq 8$, we have $s_l \leq \frac{56}{s}$ by symmetry. Now assume that $r = 7$, $s \geq 11$, And let q be the smallest prime number $q \geq 17$, such that $q \neq l$, $q \nmid rs$ and $q \nmid s_l$. Then we can porve easily that $q \nmid r, s_l$, hence we have $q \leq 23$. Then

$$s_l s \leq \max_{q \in \{17,19,23\}} \frac{a_2(q)/\log(q) + 7.6}{20/7} < 56,$$

thus $s_l \leq \frac{55}{s} < \frac{56}{s}$.

The proof of assertion (v) is similar to that of assertion (iv), cf. the computation in [37] for details. □

Lemma 4.6. Let $r \geq 7$, $s \geq 8$ be positive integers, (x, y, z) be a triple of positive coprime integers such that $\delta_r x^r + \delta_s y^s = z^3$, where $\delta_r, \delta_s \in \{\pm 1\}$. Write $r_2 \overset{\text{def}}{=} v_2(x)$, $s_2 \overset{\text{def}}{=} v_2(y)$. Then we have $r_2 \leq \frac{667}{r}$, $s_2 \leq \frac{667}{s}$.

Proof. For each prime number $p \geq 17$, write [cf. Lemma 4.1]

$$a_1(p) \overset{\text{def}}{=} 6 \cdot \frac{p^2 + 5p}{p^2 + p - 12} \cdot (1 - \frac{1}{12p}),\ a_2(p) \overset{\text{def}}{=} 6 \cdot \mathrm{Vol}(\mathfrak{R}_p^{(1)}) + a_1(p) \cdot \log(6p).$$

Then we have $6 < a_1(p) < 7.6$, and we have $a_2(17) < 978$, $a_2(19) < 1041$, $a_2(23) < 1178$, $a_2(29) < 1389$, $a_2(31) < 1475$. Moreover, we have $x_l = y_l = 1$ by Lemma 4.5.

(1) When $r_2 > 0$, let $l \geq 17$ be the smallest prime numbr such that $l \nmid rs$, $l \nmid r_2$. Following the notation of Lemma 4.1, we have $2^{3r_2 r} x_1^r \mid N_l'$ and $\log \mathrm{rad}(N) \leq \log \mathrm{rad}(6l x_1 y_1)$. Then by (4.1), we have $\log(2^{3r_2 r} x_1^{3r} y_1^s) \leq a_1(p) \cdot \log \mathrm{rad}(6l x_1 y_1) + \mathrm{Vol}(\mathfrak{R}_l^{(1)}) = a_2(p) + 7.6 \cdot \log \mathrm{rad}(x_1 y_1)$. Hence since $s \geq 8$, we have

$$\begin{aligned} a_2(l) &\geq \log(2^{3r_2 r} x_1^{3r} y_1^s) - 7.6 \cdot \log \mathrm{rad}(x_1 y_1) \\ &\geq 3r_2 r \cdot \log(2) + \sum_{p \mid x_1 y_1} (v_p(x_1^{3r} y_1^s) - 7.6) \cdot \log(p) \geq 3r_2 r \cdot \log(2). \end{aligned}$$

Hence

$$r_2 \leq \frac{a_2(l)/\log(2)}{3r}. \tag{4.8}$$

By Proposition 4.4, we have $r_2 r \cdot \log(2) \leq \log(x_r) \leq 1400$, hence $r_2 \leq \frac{1400}{7 \cdot \log(2)} < 17 \cdot 19$. Then by replacing r or s to their prime divisors ≥ 17, we have exclude at most three possible $l \geq 17$, i.e. we have $l \leq 29$, $a_2(l) < 1389$. Hence by (4.8) we have $r_2 \leq \frac{1389/\log(2)}{3r} < \frac{668}{r}$, $r_2 \leq \frac{667}{r}$.

(2) When $s_2 > 0$, if $r \geq 8$, then we have $s_2 \leq \frac{667}{s}$ by the symmetry of r, s when $r, s \geq 8$. Now assume that $r = 7$, then we have $s \geq 11$ by Lemma 4.5.

Let $l \geq 17$ be the smallest prime numbr such that $l \nmid rs$, $l \nmid s_2$. Similar to the proof of (4.5) in Lemma 4.5, we can prove that $s_2 \leq \frac{a_2(l)/\log(2)}{20s/7}$, which is parallel to the proof of (4.8). Moreover, since $r = 7 < 17$, we further have $l \leq 23$, $a_2(l) < 1178$. Hence we have $s_2 \leq \frac{a_2(l)/\log(2)}{20s/7} \leq \frac{1178/\log(2)}{20s/7} < \frac{595}{s} < \frac{667}{s}$. □

Lemma 4.7. Let $s \geq r \geq 7$ be positive integers, (x, y, z) be a triple of positive coprime integers such that $\delta_r x^r + \delta_s y^s = z^3$, where $\delta_r, \delta_s \in \{\pm 1\}$.

For each prime number $p \geq 17$, denote [cf. Lemma 4.1]

$$\begin{aligned} &a_1(p) \overset{\text{def}}{=} 6 \cdot \frac{p^2 + 5p}{p^2 + p - 12} \cdot (1 - \frac{1}{4p}), \\ &a_2(p) \overset{\text{def}}{=} 6 \cdot \mathrm{Vol}(\mathfrak{R}_p^{(2)}) + a_1(p) \cdot \log(6), 3 \cdot \mathrm{Vol}(\mathfrak{R}_p^{(3)}) + a_1(p) \cdot \log(6p)\}. \end{aligned}$$

Then we have $6 < a_1(p) < 7.6$, and we have $a_2(17) < 403$, $a_2(19) < 425$, $a_2(23) < 472$, $a_2(29) < 544$, $a_2(31) < 578$.

Let $l \geq 17$ be a prime number such that $l \nmid rs$. Write uniquely

$$x = x_1 \cdot 2^{r_2} \cdot 3^{r_3} \cdot l^{r_l} \cdot x_l^l,\ y = y_1 \cdot 2^{s_2} \cdot 3^{s_3} \cdot l^{s_l} \cdot y_l^l,$$

where $x_1, y_1, x_l, y_l, 2, 3, l$ are pairwise coprime positive integers, $r_2, s_2, r_3, s_3, r_l, s_l \geq 0$, $x_l^l = x_{(6l)}^{\langle l \rangle}$, $y_l^l = y_{(6l)}^{\langle l \rangle}$.

(i) We have $x_l = 1$, $y_l = 1$; $r_2 \leq \frac{667}{r}$, $s_2 \leq \frac{667}{s}$; $r_3 \leq \frac{153}{r}$, $s_3 \leq \frac{153}{s}$; $r_l \leq \frac{56}{r}$, $s_l \leq \frac{56}{s}$. $7 \leq r \leq 667$, and we have $x = 2^{r_2}$ when $r \geq 138$; $11 \leq s \leq 667$, and we have $y = 2^{s_2}$ when $s \geq 138$.

(ii) We have

$$(3r - a_1(l)) \cdot \log(x_1) + (s - a_1(l)) \cdot \log(y_1) \leq a_2(l),$$
$$(r - a_1(l)) \cdot \log(x_1) + (3s - a_1(l)) \cdot \log(y_1) \leq a_2(l).$$

(iii) When $3r \geq s$, we have

$$(\frac{4rs}{r+s} - a_1(l)) \cdot \log(x_1 y_1) \leq a_2(l).$$

Proof. Assertions (i) and (ii) follow from Lemma 4.5 and Lemma 4.6. Note that when $r \geq 138$, we have $r_3 = r_l = 0$. To show $x = 2^{r_2}$, it suffices to prove that $x_1 = 1$ for some $l \geq 17$, $l \nmid rs$. We can assume that each of r, s is divided by at most one prime number ≥ 17, then we can take $l \in \{17, 19, 23\}$. Hence $a_2(l) < 472$. Then $\log(x_1) < \frac{a_2(l)}{3r-7.6} < \frac{472}{3 \cdot 138 - 7.6} < \log(4)$, hence $x_1 = 1$. Then $x = 2^{r_2}$. If $r \geq 668$, then $r_2 = 0$, $x = 1$, which is impossible by Catalan's conjecture! Hence $r \leq 667$. The results concerning s can be proved similarly.

assertion (iii) is obtained by computing $(1 - \lambda) \times$ "the first inequality of (ii)" $+ \frac{13}{14} \times$ "the second inequality of (ii)", where $\lambda = \frac{3r-s}{2(r+s)}$. □

Proposition 4.8. For any positive integers (r, s), such that $r \geq 12$, $s \geq 30$, or $s > r \geq 18$, there does not exist any triple (x, y, z) of positive coprime integers satisfying $\delta_r x^r + \delta_s y^s = z^3$, where $\delta_r, \delta_s \in \{\pm 1\}$.

Proof. The proof of the proposition follows from the computation in [38], where we have $s \neq r$ since the signatures $(3, n, n)$ with $n \geq 3$ are proven. The algorithm we used is similar to the algorithm described in Remark 2.8, which is based on Lemma 4.7. □

Corollary 4.9. Suppose that (r, s, t) is a permutation of $(3, m, n)$ with $n \geq m \geq 3$, such that m, n does not satisfy one of the following conditions:

- $m \in \{4, 8, 10\}$, and $11 \leq n \leq 109$ or $n \in \{113, 121\}$.
- $m = 5$, and $7 \leq n \leq 3677$; $m \in \{7, 11\}$, and $11 \leq n \leq 667$.
- $13 \leq m \leq 17$, $m < n \leq 29$.

Then the generalized Fermat equation $x^r + y^s = z^t$ has no non-trivial primitive solution except for the solutions related to the Catalan solutions and the nine non-Catalan solutions enumerated in the introduction.

Proof. cf. Corollary 3.8, Proposition 4.4 and Proposition 4.8. □

5 Conclusion

In the last three sections, we have researched on the generalized Fermat equation

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

with signature (r, s, t) in three different cases. As a summary, we have the following result.

Theorem 5.1. 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 ($\star$) has no non-trivial primitive solution, exceplt for the solutions related to the Catalan solution $1^n + 2^3 = 3^2$ and nine non-Catalan solutions listed in the Introduction, 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 $m \geq 5$, $n \geq 7$.

Proof. The theorem follows from Propositions 2.9, Corollary 3.8, and Corollary 4.9. □

Remark 5.1.1. (i) It is worth noting that with further analysis of upper bounds and more computations for searching solutions, an expanded set of signatures including the permutations of $(4, 7, n)$, $(5, 6, n)$ are likely to be solved.

(ii) Similar to the methods in Section 4, for the generalized Fermat equations with signature $(2, m, n)$ and thier permutations, since the signature $(2, 4, n)$, $(2, n, 4)$, $(2, 5, 5)$ have been solved, we can deduce that $m, n \geq 5$ and $\max\{m, n\} \geq 7$.

By using Lemma 1.10, we can prove upper bounds for m, n similarly. A very rough estimation shows that we have $n < 2600$ for $m = 5$, and $n < 1200$ for $m \geq 7$, the related work will be undertaken in future studies.

(iii) Some of the signatures listed above can be exculded based on the proven signatures. For example, since the signatures $(2, 4, 5)$, $(4, 5, 2)$, $(4, 5, 3)$, $(2, 5, 5)$ have been solved [cf. Introduction], permutations of $(4, 5, n)$ with n a multiple of $2, 3, 5$ can also be solved, can the related generalized Fermat equation ($\star$) has no non-trivial primitive solution in this case; similarly, we can show that for permutations of $(4, 7, n)$ with n a multiple of $2, 3, 7$, and permutations of $(5, 6, n)$ with n a multiple of $2, 3, 5$, ($\star$) has no non-trivial primitive solution.

Corollary 5.2. 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.

Proof. For the case of $r, s, t \geq 4$, cf. the discussion in Remark 5.1.1, (iii). For the case of Beal conjecture and the computation of the number of unsolved signatures, cf. the computation in [37]. □

References

[1] Clemens Adelmann. *The decomposition of primes in torsion point fields*, volume 1761 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2001.

[2] Boris Bartolomé and Preda Mihăilescu. Semilocal approximation for the fermat-catalan and further popular diophantine norm equations, 2022.

[3] Michael A. Bennett and Imin Chen. Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^n$. *Algebra Number Theory*, 6(4):707–730, 2012.

[4] Michael A. Bennett, Imin Chen, Sander R. Dahmen, and Soroosh Yazdani. Generalized Fermat equations: a miscellany. *Int. J. Number Theory*, 11(1):1–28, 2015.

[5] Michael A. Bennett, Jordan S. Ellenberg, and Nathan C. Ng. The Diophantine equation $A^4 + 2^\delta B^2 = C^n$. *Int. J. Number Theory*, 6(2):311–338, 2010.

[6] Michael A. Bennett and Chris M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[7] Frits Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Math. J.*, 91(1):61–88, 1998.

[8] Wieb Bosma, John Cannon, and Catherine Steel. Magma: A system for algebra and geometry computation. *Journal of Symbolic Computation*, 24(3):235–265, 1997.

[9] David Brown. Primitive integral solutions to $x^2 + y^3 = z^{10}$. *Int. Math. Res. Not. IMRN*, (2):423–436, 2012.

[10] Nils Bruin. The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$. *Compositio Math.*, 118(3):305–321, 1999.

[11] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[12] Nils Bruin. The primitive solutions to $x^3+y^9 = z^2$. *J. Number Theory*, 111(1):179–189, 2005.

[13] Imin Chen. On the equation $s^2 + y^{2p} = \alpha^3$. *Math. Comp.*, 77(262):1223–1227, 2008.

[14] Imin Chen and Samir Siksek. Perfect powers expressible as sums of two cubes. *J. Algebra*, 322(3):638–656, 2009.

[15] Henri Cohen. *Number theory. Vol. II. Analytic and modern tools*, volume 240 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[16] Sander R. Dahmen. A refined modular approach to the Diophantine equation $x^2+y^{2n} = z^3$. *Int. J. Number Theory*, 7(5):1303–1316, 2011.

[17] Sander R. Dahmen and Samir Siksek. Perfect powers expressible as sums of two fifth or seventh powers. *Acta Arith.*, 164(1):65–100, 2014.

[18] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p+By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[19] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[20] Johnny Edwards. A complete solution to $X^2 + Y^3 + Z^5 = 0$. *J. Reine Angew. Math.*, 571:213–236, 2004.

[21] Jordan S. Ellenberg. Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. *Amer. J. Math.*, 126(4):763–787, 2004.

[22] R. Daniel Mauldin. A generalization of Fermat's last theorem: the Beal conjecture and prize problem. *Notices Amer. Math. Soc.*, 44(11):1436–1437, 1997.

[23] Preda Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.*, 572:167–195, 2004.

[24] Shinichi Mochizuki. Inter-universal Teichmüller theory I: Construction of Hodge theaters. *Publ. Res. Inst. Math. Sci.*, 57(1-2):3–207, 2021.

[25] Shinichi Mochizuki. Inter-universal Teichmüller theory II: Hodge-Arakelov-theoretic evaluation. *Publ. Res. Inst. Math. Sci.*, 57(1-2):209–401, 2021.

[26] Shinichi Mochizuki. Inter-universal Teichmüller theory III: Canonical splittings of the log-theta-lattice. *Publ. Res. Inst. Math. Sci.*, 57(1-2):403–626, 2021.

[27] Shinichi Mochizuki. Inter-universal Teichmüller theory IV: Log-volume computations and set-theoretic foundations. *Publ. Res. Inst. Math. Sci.*, 57(1-2):627–723, 2021.

[28] 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.

[29] Bjorn Poonen. Some Diophantine equations of the form $x^n + y^n = z^m$. *Acta Arith.*, 86(3):193–205, 1998.

[30] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll. Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$. *Duke Math. J.*, 137(1):103–158, 2007.

[31] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[32] Samir Siksek and Michael Stoll. Partial descent on hyperelliptic curves and the generalized Fermat equation $x^3 + y^4 + z^5 = 0$. *Bull. Lond. Math. Soc.*, 44(1):151–166, 2012.

[33] Samir Siksek and Michael Stoll. The generalised Fermat equation $x^2 + y^3 = z^{15}$. *Arch. Math. (Basel)*, 102(5):411–421, 2014.

[34] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[35] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[36] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[37] Zhong-Peng Zhou. Github Code Repository for "The inter-universal Teichmüller theory and new Diophantine results over the rational numbers. II" . Available at https://github.com/zhongpengzhou/IUT-Q-II-code.

[38] Zhong-Peng Zhou. The inter-universal Teichmüller theory and new Diophantine results over the rational numbers. I. Available as a preprint at https://arxiv.org/abs/2503.14510, 2025.

(Zhong-Peng Zhou) Institute for Theoretical Sciences, Westlake University, No. 600 Dunyu Road, Xihu District, Hangzhou, Zhejiang, 310030, P.R. China

E-mail address: zhouzhongpeng@westlake.edu.cn