Regularity criteria and an effective bound for irregular extensions of Euler triples

A. Dujella and S. Slijepčević

November 12, 2026

hexagon:2611.00431v1

Abstract

An Euler triple is a Diophantine triple $\{a, b, c\}$ with $a < b < c = a + b + 2\sqrt{ab+1}$. It extends to the regular Diophantine quadruple $\{a, b, c, d_+\}$, and it is conjectured that it has no other extension $d > c$. We prove that an irregular extension forces $c < 4 \cdot 10^{48}$, against $c < 10^{98}$ in recent work of He and Togbé. The proof squeezes the index m of the extension, which locates a common term of two Pell sequences, between a floor from congruences, $c < 8m^4$, valid for every irregular extension, and ceilings from linear forms in logarithms. The same squeeze, with other bounds, gives three regularity criteria: by the size of b/a, which confines irregular extensions to $1 + \frac{1}{1538} < b/a < 3355^2$; by pair coordinates, through the hypergeometric method; and by coprime divisors of the index combinations, which settles every Euler triple with two elements in a ratio $j : k$ with $jk \leq 300$. As applications, the three-parameter family of Cipu, Fujita and Mignotte extends only regularly when $\nu A \geq 2$ and $K \geq 643$, and when $K = 1$, $A \in \{2, 3\}$ and $\nu \geq 2$; the latter contains the Hoggatt–Bergum triples, for which this recovers Dujella's theorem for extensions $d > c$.

Contents

1 Introduction **3**
1.1 Index systems and the main results 3
1.2 Methods and plan of the paper 5

2 Euler triples, index systems and the two linear forms **6**
2.1 Euler triples and their extensions 6
2.2 The index system of an extension 8
2.3 The index ordering and the two linear forms 14

3 A quartic index floor **19**

4 Close Pell units force regularity **24**

5 Regularity from pair coordinates **31**
5.1 Rickert's approximants and Bennett's criterion 31
5.2 An approximation measure for a pair representation 37
5.3 The index in pair coordinates 43

6 Coprime divisors of the index combinations **48**

7 An effective bound for irregular extensions **51**
7.1 The a priori bound 51
7.2 Index caps on windows of c 53

8 Families of Euler triples that extend only regularly **60**
8.1 The three-parameter Fibonacci family 60
8.2 Euler triples of small ratio type 63

A The three-parameter family for $643 \le K \le 2401$ **65**

B A Baker–Davenport reduction for a single Euler triple **69**

1 Introduction

A set of positive integers is a *Diophantine tuple* if the product of any two of its elements, increased by 1, is a perfect square. Every Diophantine triple $\{a, b, c\}$ with $a < b < c$, where $ab + 1 = r^2$, $ac + 1 = s^2$ and $bc + 1 = t^2$, extends to the Diophantine quadruple $\{a, b, c, d_+\}$, where

$$d_+ = d_+(a, b, c) = a + b + c + 2abc + 2rst,$$

as observed by Arkin, Hoggatt and Straus [3] and, independently, by Gibbs (see [15]). An integer $d > c$ such that $\{a, b, c, d\}$ is a Diophantine quadruple is an *extension* of the triple; it is *regular* if $d = d_+(a, b, c)$ and *irregular* otherwise. The regularity conjecture, which goes back to the same authors, asserts that every Diophantine quadruple is regular, that is, that every extension of a Diophantine triple is regular (see [18]). It implies that there is no Diophantine quintuple: Dujella proved that there are only finitely many [14], and He, Togbé and Ziegler that there are none [19]. For a fixed triple, Fujita and Miyazaki [18] showed that there are at most eleven extensions, and Cipu, Fujita and Miyazaki [11] that there are at most eight. In a recent preprint He and Togbé [20] give a proof that there are only finitely many irregular Diophantine quadruples. The conjecture itself is open.

This paper is about the extensions of *Euler triples*, the Diophantine triples $\{a, b, c\}$ with $a < b < c$ and

$$c = a + b + 2r, \qquad r = \sqrt{ab + 1}$$

(Definition 2.3). The name is that of He, Togbé and Ziegler [19]; Cipu, Fujita and Mignotte [7] and Dujella [15] call these triples regular, a word that in this paper qualifies only extensions. By a lemma of Jones [21] (see [19]), a Diophantine triple with $a < b < c$ either is an Euler triple or satisfies $c > 4ab$. So each Diophantine pair $\{a, b\}$ with $a < b$ lies in exactly one Euler triple with third element larger than b, and among the Diophantine triples that contain the pair as their two smallest elements it has the least third element. For an Euler triple, $s = a + r$, $t = b + r$ and $d_+(a, b, c) = 4rst$ (Lemma 2.4), and we write

$$\alpha = r + \sqrt{ab}, \qquad \beta = s + \sqrt{ac}, \qquad \gamma = t + \sqrt{bc}$$

for its units. Cipu, Fujita and Miyazaki [11] showed that an Euler triple has at most three extensions $d > d_+(a, b, c)$.

1.1 Index systems and the main results

Let d be an *irregular extension* of an Euler triple $\{a, b, c\}$, that is, an integer $d > c$ with $d \neq d_+(a, b, c)$ such that $\{a, b, c, d\}$ is a Diophantine quadruple, and write $ad+1 = x^2$, $bd+1 = y^2$ and $cd+1 = z^2$ with $x, y, z > 0$. An *index system* of d (Definition 2.5) is a quadruple (λ, l, m, n), with $\lambda \in \{-1, 1\}$ and integers $l, m, n \geq 0$, such that

$$y\sqrt{a} + x\sqrt{b} = (\sqrt{a} + \sqrt{b})\,\alpha^{2l}, \qquad z\sqrt{a} + x\sqrt{c} = (\lambda\sqrt{a} + \sqrt{c})\,\beta^{2m},$$
$$z\sqrt{b} + y\sqrt{c} = (\lambda\sqrt{b} + \sqrt{c})\,\gamma^{2n}.$$

By Proposition 2.11, every extension has exactly one index system, and by Lemma 2.14 the index system of an irregular extension satisfies $3 \leq n < m < l < 2n$; we call m the *index* of the extension. It locates z as a common term of the Pell sequences of the pairs $\{a, c\}$ and $\{b, c\}$, at the positions m and n (Lemma 2.8). Each of our results compares a lower bound for the index, coming from the arithmetic of the three representations, with an upper bound coming from Diophantine approximation. The first result is a universal lower bound.

Index floor (Theorem 3.6). *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$. Then $c < 4m^2(m+\lambda)^2 < 8m^4$.*

Equivalently, $m > (c/8)^{1/4}$: the index grows at least like the fourth root of c. The previous lower bound for the index of an Euler triple, $32m^5 > c \log c$ for $c \geq 10^7$ [20], gives $m > (c \log c/32)^{1/5}$, a fifth root; Theorem 3.6 raises the exponent of c from $1/5$ to $1/4$ and needs no condition on c. We do not know whether the exponent $1/4$ is optimal. The index floor is the heart of the paper: it is the lower bound behind the pair-coordinate criterion, the effective bound and the three-parameter family below.

Two of the units α, β, γ are close when b/a is large, and when $b - a$ is small compared with $\sqrt{ac}$. In both cases the three representations force regularity.

Close Pell units (Theorem 4.5). *Let $\{a, b, c\}$ be an Euler triple with $b \geq 3355^2 a$ or $\sqrt{ac} \geq 3075\,(b-a)$. Then $\{a, b, c\}$ has no irregular extension.*

Consequently an Euler triple with an irregular extension satisfies $1 + \frac{1}{1538} < b/a < 3355^2$ (Corollary 4.6). The second condition holds whenever $b - a \leq a/1538$; for Euler triples with $a > 3.8 \cdot 10^7$ this range contains the range $b < a + 4\sqrt{a}$ of the close-pair theorem of Filipin, Fujita and Togbé [17]. The constants come from one numerical inequality in Laurent's bound for linear forms in two logarithms [22], which they satisfy with a margin below one half of one percent. In their concluding remarks Cipu, Fujita and Mignotte [7] explain that their two-parameter families became tractable through sharp bounds for the difference of the integer coefficients of the logarithms, and write that "it remains for future works to obtain similar bounds for general triples, not necessarily given parametrically". For Euler triples such bounds are the gap inequalities

$$m > (l-m)\,R_x, \qquad n > (m-n)\,R_z, \qquad \text{where} \quad R_x = \sqrt{\frac{b}{a}}\,\log\alpha, \quad R_z = \frac{\sqrt{ac}}{b-a}\,\log\beta$$

(Lemma 2.18), and Theorem 4.5 follows from them and Laurent's theorem.

The third criterion uses coordinates adapted to the hypergeometric method. A *pair representation* of sign $\sigma \in \{-1, 1\}$ of an Euler triple $\{a, b, c\}$ is a quadruple (p_1, q_1, p_2, q_2) of positive integers with $a = p_1 q_1$, $b = p_2 q_2$ and $p_1 q_2 - p_2 q_1 = 2\sigma$ (Definition 5.8). Every Euler triple has one, and its *pair coordinates* (p_1, q_1), (p_2, q_2) and $(p_3, q_3) = (p_1 + p_2, q_1 + q_2)$ satisfy $c = p_3 q_3$ (Lemma 5.10).

Pair coordinates (Theorem 5.19). *Let $\{a, b, c\}$ be an Euler triple with a pair representation such that $p_1 q_3 \geq 800\,p_3^2$, or such that $p_1 q_3 \geq 42\,p_3^2$ and $c \geq 4.5 \cdot 10^{12}$. Then $\{a, b, c\}$ has no irregular extension.*

Cipu, Fujita and Mignotte [10] proved the regularity of a three-parameter family of Euler triples by the simultaneous approximations of Rickert [26] and the criterion of Bennett [6], under a growth condition on the parameters. Their approximation measure extends to every pair representation with $p_1 q_3 \geq 168$ (Theorem 5.14). Together with the index floor, which takes the place of their congruence lower bound for the index, it gives Theorem 5.19; on their family it removes the growth condition.

The fourth criterion is arithmetic. For an Euler triple put

$$\Delta_{ab} = \frac{\gcd(a,b)}{\gcd(a,b,4)}, \qquad \Delta_{bc} = \frac{\gcd(b,c)}{\gcd(b,c,4)}, \qquad \Delta_{ac} = \frac{\gcd(a,c)}{\gcd(a,c,4)},$$
$$G_{rc} = \frac{\gcd(r,c)}{\gcd(r,c,2)}, \qquad G_{ta} = \frac{\gcd(t,a)}{\gcd(t,a,2)}, \qquad G_{sb} = \frac{\gcd(s,b)}{\gcd(s,b,2)},$$

and call $\Pi_1 = \Delta_{ab}G_{rc}$, $\Pi_2 = \Delta_{bc}G_{ta}$ and $\Pi_3 = \Delta_{ac}G_{sb}$ its *coprime divisors* (Definition 6.1); the two factors of each product are coprime (Lemma 6.2). The *index combinations* of an index system are $m - n$, $l + \lambda m$ and $l + \lambda n$.

Coprime divisors (Theorem 6.3). *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$, with the coprime divisors Π_1, Π_2, Π_3 and the gap ratio R_z above. Then*

$$\Pi_1 \mid m - n, \qquad \Pi_2 \mid l + \lambda m, \qquad \Pi_3 \mid l + \lambda n, \qquad \text{and} \qquad m > \Pi_1(1 + R_z).$$

The application is to Euler triples with two elements in a fixed ratio, for which the coprime divisors grow linearly with c. An Euler triple has *ratio type* $j : k$, for coprime integers $1 \le j < k$, if two of its elements $v < w$ satisfy $jw = kv$ (Definition 8.5); for each $j : k$ and each choice of the two positions, these triples come from the positive solutions of the Pell equation $u^2 - jkg^2 = 1$ (Lemma 8.6).

Fixed ratios (Theorem 8.7). *Let $\{a, b, c\}$ be an Euler triple of ratio type $j : k$. If $\{a, b, c\}$ has an irregular extension, then*

$$\frac{c}{6(j+k)} - 0.15 < 2.4638 \cdot 10^{12} (\log c)^2 \log \frac{19.46\, c}{6(j+k)}.$$

If $jk \le 300$, then $\{a, b, c\}$ has no irregular extension.

Earlier results of this kind concern single ratios; they are listed in the table at the head of Section 8.

Finally, all irregular extensions of Euler triples are confined to an explicit range.

Effective bound (Theorem 7.9). *Let $\{a, b, c, d\}$ be a Diophantine quadruple with $a < b < c < d$ and $c = a + b + 2\sqrt{ab + 1}$. If $d \ne d_+(a, b, c)$, then $c < 4 \cdot 10^{48}$.*

This improves the bound $c < 10^{98}$ of [20]. Near the new bound the index floor forces the index m to be of order 10^{12}.

As applications we settle two subfamilies of the three-parameter family of Cipu, Fujita and Mignotte [10]. With $F_{-1} = 1$, $F_0 = 0$ and $F_{k+2} = F_{k+1} + F_k$, integers $\nu, A, K \ge 1$ and a sign $\varepsilon \in \{-1, 1\}$, put $\phi_k = F_k A + F_{k-1}$ and $f_k = \phi_k(\phi_k K + 2\varepsilon F_k)$; the *family triple* of the parameter point (ν, A, K, ε) is $\{f_\nu, f_{\nu+1}, f_{\nu+2}\}$ (Convention 8.1), an Euler triple for $K \ge 3$ (Lemma 8.2). We prove that the family triple has no irregular extension when $\nu A \ge 2$ and either $K \ge 643$, or $K \ge 128$ and $c \ge 4.5 \cdot 10^{12}$ (Corollary 8.3), and when $K = 1$, $A \in \{2, 3\}$ and $\nu \ge 2$ (Theorem 8.4). For $(A, \varepsilon) = (3, -1)$ the family triples are the Hoggatt–Bergum triples $\{F_{2\nu+2}, F_{2\nu+4}, F_{2\nu+6}\}$, and for extensions $d > c$ Theorem 8.4 recovers Dujella's theorem on them [12]; these triples are also covered by the results of Filipin, Fujita and Togbé [17] on the pairs $\{F_{2k}, F_{2k+2}\}$ and of Park and Lee [25] on the pairs $\{F_{2k}, F_{2k+4}\}$. The table at the head of Section 8 compares these applications, and the other families settled here, with what was known.

1.2 Methods and plan of the paper

The lower bounds are arithmetic. Expanding the three Pell sequences at their common terms to second order, by the congruences of Dujella [13], and to third order, following He and Togbé [20], gives congruences for l, m, n modulo a, b and c, and integer combinations of them in which the leading terms cancel give the index floor. Reducing the multiplication matrices modulo the gcds of two elements, or of a root and an element, gives the divisibilities behind the coprime divisors, and the divisibility of a quadratic index form in pair coordinates gives a further lower

bound in the pair-coordinate criterion; for close units the gap inequalities play the part of the lower bound. The upper bounds are analytic. Those from linear forms in logarithms start from the two linear forms

$$\Lambda_x = 2l\log\alpha - 2m\log\beta + \log D_\lambda, \qquad \Lambda_z = 2m\log\beta - 2n\log\gamma + \log E_\lambda$$

of Definition 2.16, with explicit algebraic numbers D_λ, E_λ, which satisfy $0 < \Lambda_x < 4.01\,\beta^{-4m}$ and $0 < \Lambda_z < 2\,\beta^{-4n}$ (Lemma 2.18). They are bounded from below by Laurent's theorem on linear forms in two logarithms [22] for close units, by Matveev's theorem [23] for the a priori bound (Proposition 7.3), and by the theorem of Mignotte and Voutier [24] on linear forms in three logarithms for the effective bound. For pair coordinates the upper bound comes from the approximants of Rickert [26], with Bennett's criterion [6] and the prime product of Cipu and Fujita [9]. Individual triples below the analytic thresholds are closed by the reduction of Baker and Davenport [4] in the form of Dujella and Pethő [16] (Proposition B.1). Several steps of the proofs are finite computations: numerical inequalities certified in interval arithmetic with outward rounding, exhaustive checks over explicit finite sets, and these reductions. Each is stated where it is used, with what it checks and how.

Section 2 contains the common setting: Euler triples, their index systems and the two linear forms. Its results are used throughout, above all the existence and uniqueness of the index system (Proposition 2.11) and the ordering of the indices (Lemma 2.14), on which every later section rests. The index floor, the criteria for close units, pair coordinates and coprime divisors, and the effective bound are proved in Sections 3 to 7, in this order. After Section 2, Sections 3, 4 and 6 can be read independently of one another; Section 5 uses the index floor, and Section 7 uses the index floor and the heights and Laurent's theorem of Section 4. Section 8 proves the results on fixed ratios and on the three-parameter family, with a table comparing them with the literature. Appendix A contains the proof for the three-parameter family with $643 \le K \le 2401$, and Appendix B the reduction for a single triple.

2 Euler triples, index systems and the two linear forms

This section sets up the objects of the paper and proves the facts on which the later sections rest: every extension of an Euler triple has exactly one index system (Proposition 2.11), and for an irregular extension the indices are ordered (Lemma 2.14) and the two linear forms Λ_x and Λ_z are exponentially small in the index (Lemma 2.18). Most of it is routine or quoted. The one step that carries an idea is the comparison of two expressions of one number (Lemma 2.17), which gives both linear forms their smallness.

2.1 Euler triples and their extensions

Definition 2.1. A **Diophantine tuple** is a finite set of distinct positive integers in which the product of any two distinct elements, increased by 1, is a perfect square. A Diophantine tuple with three elements is a **Diophantine triple**, and one with four elements is a **Diophantine quadruple**.

Definition 2.2. Let $\{a, b, c\}$ be a Diophantine triple (Definition 2.1) with $a < b < c$, and put

$$d_\pm(a,b,c) = a + b + (2ab+1)c \pm 2\sqrt{(ab+1)(ac+1)(bc+1)}.$$

An **extension** of $\{a, b, c\}$ is an integer $d > c$ such that $\{a, b, c, d\}$ is a Diophantine quadruple. The extension d is **regular** if $d = d_+(a, b, c)$ and **irregular** otherwise. A Diophantine quadruple

$\{a,b,c,d\}$ with $a<b<c<d$ is **regular** or **irregular** according as d is a regular or an irregular extension of $\{a,b,c\}$.

Definition 2.3. An **Euler triple** is a set $\{a,b,c\}$ of positive integers $a<b<c$ such that $ab+1=r^2$ for a positive integer r and

$$c=a+b+2r.$$

Its **roots** are r, $s=a+r$ and $t=b+r$. Its **units** are

$$\alpha=r+\sqrt{ab},\qquad \beta=s+\sqrt{ac},\qquad \gamma=t+\sqrt{bc},$$

and its **multiplication matrices** are

$$\mathbf{A}=\begin{pmatrix} r & b\\ a & r\end{pmatrix},\qquad \mathbf{B}=\begin{pmatrix} s & c\\ a & s\end{pmatrix},\qquad \mathbf{C}=\begin{pmatrix} t & c\\ b & t\end{pmatrix}.$$

Lemma 2.4. *Let $\{a,b,c\}$ be an Euler triple with roots r,s,t, units α,β,γ and multiplication matrices $\mathbf{A},\mathbf{B},\mathbf{C}$ (Definition 2.3). Then:*

1. *$ac+1=s^2$ and $bc+1=t^2$; in particular $\{a,b,c\}$ is a Diophantine triple;*
2. *$cr-st=rs-at=rt-bs=1$, and $d_+(a,b,c)=4rst=4r(cr-1)$;*
3. *r,s,t are pairwise coprime, and $\gcd(a,r)=\gcd(a,s)=\gcd(b,t)=1$;*
4. *$b-a\geq 2$, $b\geq 3$, $a<r<b$ and $4a<c\leq 2(a+b)$;*
5. *none of ab,ac,bc is a perfect square; $\det\mathbf{A}=\det\mathbf{B}=\det\mathbf{C}=1$, and $\alpha^{-1}=r-\sqrt{ab}$, $\beta^{-1}=s-\sqrt{ac}$, $\gamma^{-1}=t-\sqrt{bc}$; for integers u,v,*

$$(u\sqrt{a}+v\sqrt{b})\,\alpha=u_1\sqrt{a}+v_1\sqrt{b},\qquad (u\sqrt{a}+v\sqrt{c})\,\beta=u_2\sqrt{a}+v_2\sqrt{c},$$
$$(u\sqrt{b}+v\sqrt{c})\,\gamma=u_3\sqrt{b}+v_3\sqrt{c},$$

   where $\binom{u_1}{v_1}=\mathbf{A}\binom{u}{v}$, $\binom{u_2}{v_2}=\mathbf{B}\binom{u}{v}$, $\binom{u_3}{v_3}=\mathbf{C}\binom{u}{v}$;
6. *$\mathbf{B}\binom{-1}{1}=\binom{t}{r}$, $\mathbf{B}^{-1}\binom{1}{1}=\binom{-t}{r}$, $\mathbf{C}\binom{-1}{1}=\binom{s}{r}$ and $\mathbf{C}^{-1}\binom{1}{1}=\binom{-s}{r}$.*

Proof. Throughout, $c=a+b+2r$, $s=a+r$, $t=b+r$ and $r^2=ab+1$.

We first prove items 1 and 2. One has $s^2=a^2+2ar+ab+1=a(a+b+2r)+1=ac+1$, and in the same way $t^2=bc+1$; with $ab+1=r^2$ this shows that $\{a,b,c\}$ is a Diophantine triple (Definition 2.1). Next,

$$cr-st=r(a+b)+2r^2-ab-r(a+b)-r^2=r^2-ab=1,$$

$$rs-at=ra+r^2-ab-ar=1,\qquad rt-bs=rb+r^2-ab-br=1.$$

By Definition 2.2 and item 1, $d_+(a,b,c)=a+b+(2ab+1)c+2rst$. Using $a+b=c-2r$, $2ab+1=2r^2-1$ and $cr-1=st$,

$$d_+(a,b,c)=c-2r+(2r^2-1)c+2rst=2r(cr-1+st)=4rst=4r(cr-1).$$

We next prove item 3. A common divisor of r and s divides $rt - bs = 1$; a common divisor of r and t, or of s and t, divides $rs - at = 1$; a common divisor of a and r divides $rs - at = 1$. Finally $s^2 - ac = 1$ and $t^2 - bc = 1$ give $\gcd(a, s) = \gcd(b, t) = 1$.

We next prove item 4. If $b = a + 1$, then $a^2 < ab + 1 = a^2 + a + 1 < (a + 1)^2$, so $ab + 1$ is not a square; hence $b - a \geq 2$ and $b \geq 3$. Since $r^2 = ab + 1 > a^2$, $r > a$; since $a \leq b - 1$, $r^2 \leq b^2 - b + 1 < b^2$, so $r < b$. Then $c = a + b + 2r > a + a + 2a = 4a$. Finally $(a + b)^2 - 4r^2 = (b - a)^2 - 4 \geq 0$, so $2r \leq a + b$ and $c \leq 2(a + b)$.

We next prove item 5. Since $r > a \geq 1$, $r \geq 2$ and $(r - 1)^2 < r^2 - 1 = ab < r^2$, so ab is not a square; likewise $ac = s^2 - 1$ and $bc = t^2 - 1$ with $s, t \geq 3$. The determinants are $r^2 - ab$, $s^2 - ac$, $t^2 - bc$, all equal to 1 by $r^2 = ab + 1$ and item 1, and $(r + \sqrt{ab})(r - \sqrt{ab}) = r^2 - ab = 1$, and likewise for β, γ. Expanding,

$$\begin{aligned}(u\sqrt{a} + v\sqrt{b})(r + \sqrt{ab}) &= (ru + bv)\sqrt{a} + (au + rv)\sqrt{b},\\ (u\sqrt{a} + v\sqrt{c})(s + \sqrt{ac}) &= (su + cv)\sqrt{a} + (au + sv)\sqrt{c},\\ (u\sqrt{b} + v\sqrt{c})(t + \sqrt{bc}) &= (tu + cv)\sqrt{b} + (bu + tv)\sqrt{c},\end{aligned}$$

which are the matrix products of item 5. Since ab is not a square, $\sqrt{a}$ and $\sqrt{b}$ are linearly independent over $\mathbb{Q}$, so the coordinates in the first display are unique; likewise for the pairs $\sqrt{a}, \sqrt{c}$ and $\sqrt{b}, \sqrt{c}$.

We finally prove item 6. Since $c - s = b + r = t$, $s - a = r$, $c - t = a + r = s$ and $t - b = r$,

$$\mathbf{B}\begin{pmatrix}-1\\1\end{pmatrix} = \begin{pmatrix}c - s\\ s - a\end{pmatrix} = \begin{pmatrix}t\\r\end{pmatrix}, \qquad \mathbf{B}^{-1}\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}s & -c\\ -a & s\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}-t\\r\end{pmatrix},$$

$$\mathbf{C}\begin{pmatrix}-1\\1\end{pmatrix} = \begin{pmatrix}c - t\\ t - b\end{pmatrix} = \begin{pmatrix}s\\r\end{pmatrix}, \qquad \mathbf{C}^{-1}\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}t & -c\\ -b & t\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}-s\\r\end{pmatrix},$$

where $\mathbf{B}^{-1}$ and $\mathbf{C}^{-1}$ are the adjugates because the determinants are 1. □

2.2 The index system of an extension

An extension d of an Euler triple gives one solution of the Pell equation of each pair of the triple, and the index system records where these solutions lie in the orbits of the units.

Definition 2.5. Let d be an extension (Definition 2.2) of an Euler triple $\{a, b, c\}$ with units α, β, γ (Definition 2.3), and let x, y, z be the positive integers with

$$ad + 1 = x^2, \qquad bd + 1 = y^2, \qquad cd + 1 = z^2.$$

An **index system** of d is a quadruple (λ, l, m, n), where $\lambda \in \{-1, 1\}$ and $l, m, n \geq 0$ are integers, such that

$$y\sqrt{a} + x\sqrt{b} = (\sqrt{a} + \sqrt{b})\,\alpha^{2l}, \qquad z\sqrt{a} + x\sqrt{c} = (\lambda\sqrt{a} + \sqrt{c})\,\beta^{2m}, \qquad z\sqrt{b} + y\sqrt{c} = (\lambda\sqrt{b} + \sqrt{c})\,\gamma^{2n}.$$

The integer m is the **index** of the index system. The **Pell equation of the pair** $\{a, b\}$ is the equation $ay^2 - bx^2 = a - b$ in the unknowns x, y; likewise the Pell equation of $\{a, c\}$ is $az^2 - cx^2 = a - c$, and that of $\{b, c\}$ is $bz^2 - cy^2 = b - c$.

By Proposition 2.11 below, every extension has exactly one index system, so we speak of the index system and the index of an extension. The pair (x, y) solves the Pell equation of $\{a, b\}$, since $ay^2 - bx^2 = a(bd + 1) - b(ad + 1) = a - b$; likewise (x, z) and (y, z) solve those of $\{a, c\}$ and $\{b, c\}$. The second and third displays say that $z = V_m^\lambda = W_n^\lambda$ (Lemma 2.8), with the Pell sequences of the following convention; in the notation of Dujella [13] and of Fujita and Miyazaki [18] this reads $z = v_{2m} = w_{2n}$.

Convention 2.6. Let $\{a,b,c\}$ be an Euler triple with multiplication matrices $\mathbf{B},\mathbf{C}$ (Definition 2.3). For $\lambda\in\{-1,1\}$ and integers $j\ge 0$, the **Pell sequences** V_j^{λ} and W_j^{λ} are the first coordinates of the integer vectors

$$\mathbf{B}^{2j}\begin{pmatrix}\lambda\\1\end{pmatrix}\qquad\text{and}\qquad\mathbf{C}^{2j}\begin{pmatrix}\lambda\\1\end{pmatrix},$$

respectively.

Lemma 2.7. *Let P,Q,S be positive integers with $PQ+1=S^2$, put $\eta_{PQ}=S+\sqrt{PQ}$, and let $u_0,v_0\in\mathbb{Z}$. For $j\ge 0$ let $u_j,v_j\in\mathbb{Z}$ be defined by*

$$u_j\sqrt{P}+v_j\sqrt{Q}=(u_0\sqrt{P}+v_0\sqrt{Q})\,\eta_{PQ}^{j}.$$

1. *The even subsequences satisfy $X_{i+1}=(4PQ+2)X_i-X_{i-1}$ for $i\ge 1$, where $X_i=u_{2i}$ or $X_i=v_{2i}$.*
2. *For every integer $i\ge 0$,*

$$\begin{aligned}u_{2i}&\equiv u_0+2Qi\,(Pi\,u_0+S\,v_0)\pmod{8PQ^2},\\ v_{2i}&\equiv v_0+2Pi\,(Qi\,v_0+S\,u_0)\pmod{8P^2Q}.\end{aligned}$$

Proof. This is the second-order congruence of Dujella (see [15]), in a form symmetric in the two square roots; we give the induction.

Since $PQ=S^2-1$ with $S\ge 2$, PQ is not a square, so $\sqrt{P}$ and $\sqrt{Q}$ are linearly independent over $\mathbb{Q}$ and u_j,v_j are well defined; explicitly $u_{j+1}=Su_j+Qv_j$ and $v_{j+1}=Pu_j+Sv_j$.

We first prove item 1. Since $\eta_{PQ}^{-1}=S-\sqrt{PQ}$, one has $\eta_{PQ}^{2}+\eta_{PQ}^{-2}=2(2PQ+1)=4PQ+2$, hence $\eta_{PQ}^{2(i+1)}=(4PQ+2)\eta_{PQ}^{2i}-\eta_{PQ}^{2(i-1)}$. Multiplying by $u_0\sqrt{P}+v_0\sqrt{Q}$ and comparing the coefficients of $\sqrt{P}$ and $\sqrt{Q}$ gives item 1.

We next prove item 2. Put $T=PQ$ and write $\eta_{PQ}^{2i}=U_i+K_i\sqrt{T}$ with $U_i,K_i\in\mathbb{Z}$. Expanding $(u_0\sqrt{P}+v_0\sqrt{Q})(U_i+K_i\sqrt{PQ})$ gives

$$u_{2i}=u_0U_i+Qv_0K_i,\qquad v_{2i}=v_0U_i+Pu_0K_i. \tag{1}$$

From $\eta_{PQ}^{2i+2}=\eta_{PQ}^{2i}\big((2T+1)+2S\sqrt{T}\big)$ one gets $U_{i+1}=(2T+1)U_i+2STK_i$ and $K_{i+1}=(2T+1)K_i+2SU_i$, with $U_0=1$, $K_0=0$. By induction $K_i=SJ_i$ with $J_i\in\mathbb{Z}$, where $J_0=0$ and, using $S^2=T+1$,

$$J_{i+1}=(2T+1)J_i+2U_i,\qquad U_{i+1}=(2T+1)U_i+2T(T+1)J_i.$$

We claim that

$$U_i\equiv 1+2i^2T\pmod{8T^2},\qquad J_i\equiv 2i\pmod{8T}. \tag{2}$$

This holds for $i=0$. If $U_i=1+2i^2T+8T^2g$ and $J_i=2i+8Th$ with $g,h\in\mathbb{Z}$, then

$$J_{i+1}=2(i+1)+4i(i+1)T+8T\,(h+2Th+2Tg),$$

$$U_{i+1}=1+2(i+1)^2T+4i(i+1)T^2+8T^2\,(g+2Tg+2h+2Th),$$

and $8\mid 4i(i+1)$, which proves (2) for $i+1$.

By (1) and (2),

$$u_{2i} - u_0 - 2Qi(Piu_0 + Sv_0) = u_0\big(U_i - 1 - 2i^2PQ\big) + QSv_0\big(J_i - 2i\big),$$

where the first term is divisible by $8T^2 = 8P^2Q^2$ and the second by $8QT = 8PQ^2$. Likewise

$$v_{2i} - v_0 - 2Pi(Qiv_0 + Su_0) = v_0\big(U_i - 1 - 2i^2PQ\big) + PSu_0\big(J_i - 2i\big) \equiv 0 \pmod{8P^2Q}.$$

□

Lemma 2.8. *Let $\{a, b, c\}$ be an Euler triple with roots r, s, t, units α, β, γ and multiplication matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}$ (Definition 2.3), and let $\lambda \in \{-1, 1\}$.*

1. *For every integer $k \geq 0$, the vectors $\mathbf{A}^k\binom{1}{1}$, $\mathbf{B}^k\binom{\lambda}{1}$ and $\mathbf{C}^k\binom{\lambda}{1}$ are the coordinate vectors of $(\sqrt{a} + \sqrt{b})\,\alpha^k$ with respect to $\sqrt{a}, \sqrt{b}$, of $(\lambda\sqrt{a} + \sqrt{c})\,\beta^k$ with respect to $\sqrt{a}, \sqrt{c}$, and of $(\lambda\sqrt{b} + \sqrt{c})\,\gamma^k$ with respect to $\sqrt{b}, \sqrt{c}$. Equivalently, they are the vectors $\binom{u_k}{v_k}$ of Lemma 2.7 for $(P, Q, S, u_0, v_0) = (a, b, r, 1, 1)$, $(a, c, s, \lambda, 1)$ and $(b, c, t, \lambda, 1)$, respectively.*

2. *Let d be an extension of $\{a, b, c\}$, let x, y, z be as in Definition 2.5, and let $l, m, n \geq 0$ be integers. The first, second and third displays of Definition 2.5 hold if and only if, respectively,*

$$\binom{y}{x} = \mathbf{A}^{2l}\binom{1}{1}, \qquad \binom{z}{x} = \mathbf{B}^{2m}\binom{\lambda}{1}, \qquad \binom{z}{y} = \mathbf{C}^{2n}\binom{\lambda}{1}.$$

   In particular, if (λ, l, m, n) is an index system of d, then $z = V_m^\lambda = W_n^\lambda$, with the Pell sequences of Convention 2.6.

3. *For every integer $j \geq 1$,*

$$\mathbf{A}^{2j+2}\binom{1}{1} = (4ab + 2)\,\mathbf{A}^{2j}\binom{1}{1} - \mathbf{A}^{2j-2}\binom{1}{1},$$
$$\mathbf{B}^{2j+2}\binom{\lambda}{1} = (4ac + 2)\,\mathbf{B}^{2j}\binom{\lambda}{1} - \mathbf{B}^{2j-2}\binom{\lambda}{1},$$
$$\mathbf{C}^{2j+2}\binom{\lambda}{1} = (4bc + 2)\,\mathbf{C}^{2j}\binom{\lambda}{1} - \mathbf{C}^{2j-2}\binom{\lambda}{1}.$$

   In particular the Pell sequences satisfy $V_{j+1}^\lambda = (4ac + 2)V_j^\lambda - V_{j-1}^\lambda$ and $W_{j+1}^\lambda = (4bc + 2)W_j^\lambda - W_{j-1}^\lambda$ for $j \geq 1$, and their initial terms are

$$V_0^\lambda = W_0^\lambda = \lambda, \qquad V_1^\lambda = \lambda(2ac + 1) + 2sc, \qquad W_1^\lambda = \lambda(2bc + 1) + 2tc.$$

   Both coordinates of $\mathbf{B}^{2j}\binom{\lambda}{1}$ and both coordinates of $\mathbf{C}^{2j}\binom{\lambda}{1}$ are strictly increasing in $j \geq 0$ and positive for $j \geq 1$.

Proof. Item 1 is item 5 of Lemma 2.4, applied k times; items 2 and 3 follow from it, the recurrences by item 1 of Lemma 2.7 and the monotonicity by induction.

We first prove item 1. By Lemma 2.4, item 5, ab is not a square, so $\sqrt{a}$ and $\sqrt{b}$ are linearly independent over $\mathbb{Q}$ and an element $u\sqrt{a} + v\sqrt{b}$ with $u, v \in \mathbb{Z}$ has a unique coordinate vector $\binom{u}{v}$; by the same item, multiplication by α sends the element with coordinate vector $\binom{u}{v}$ to the element with coordinate vector $\mathbf{A}\binom{u}{v}$. Induction on k shows that $\mathbf{A}^k\binom{1}{1}$ is the coordinate vector

of $(\sqrt{a}+\sqrt{b})\,\alpha^k$. In the same way, since ac and bc are not squares (same item), $\mathbf{B}^k\binom{\lambda}{1}$ and $\mathbf{C}^k\binom{\lambda}{1}$ are the coordinate vectors of $(\lambda\sqrt{a}+\sqrt{c})\,\beta^k$ and $(\lambda\sqrt{b}+\sqrt{c})\,\gamma^k$. Finally $ab+1=r^2$ (Definition 2.3), $ac+1=s^2$ and $bc+1=t^2$ (Lemma 2.4, item 1), so $(P,Q,S)=(a,b,r)$, (a,c,s) and (b,c,t) satisfy the hypothesis of Lemma 2.7, with $\eta_{PQ}=\alpha$, β and γ; and its defining identity $u_k\sqrt{P}+v_k\sqrt{Q}=(u_0\sqrt{P}+v_0\sqrt{Q})\,\eta_{PQ}^k$ says that $\binom{u_k}{v_k}$ is the coordinate vector just described.

We next prove item 2. By item 1, the right side $(\sqrt{a}+\sqrt{b})\,\alpha^{2l}$ of the first display of Definition 2.5 has coordinate vector $\mathbf{A}^{2l}\binom{1}{1}$, and its left side $y\sqrt{a}+x\sqrt{b}$ has coordinate vector $\binom{y}{x}$. Since coordinates with respect to $\sqrt{a},\sqrt{b}$ are unique, the first display holds if and only if $\binom{y}{x}=\mathbf{A}^{2l}\binom{1}{1}$. In the same way the second display holds if and only if $\binom{z}{x}=\mathbf{B}^{2m}\binom{\lambda}{1}$, and the third if and only if $\binom{z}{y}=\mathbf{C}^{2n}\binom{\lambda}{1}$. If (λ,l,m,n) is an index system of d, the first coordinates of the last two identities are $z=V_m^\lambda$ and $z=W_n^\lambda$, by Convention 2.6.

We next prove the recurrences of item 3. By item 1, the two coordinates of $\mathbf{A}^{2j}\binom{1}{1}$, of $\mathbf{B}^{2j}\binom{\lambda}{1}$ and of $\mathbf{C}^{2j}\binom{\lambda}{1}$ are the terms u_{2j} and v_{2j} of Lemma 2.7 for $PQ=ab$, ac and bc, respectively. By item 1 of Lemma 2.7, each of them satisfies $X_{j+1}=(4PQ+2)X_j-X_{j-1}$ for $j\geq 1$, which gives the three vector recurrences; their first coordinates for $\mathbf{B}$ and $\mathbf{C}$ are the recurrences of V_j^λ and W_j^λ (Convention 2.6).

We next compute the initial terms. Since $\mathbf{B}^0$ and $\mathbf{C}^0$ are the identity matrix, $V_0^\lambda=W_0^\lambda=\lambda$. Next $\mathbf{B}\binom{\lambda}{1}=\binom{\lambda s+c}{\lambda a+s}$, and, by $s^2=ac+1$,

$$\mathbf{B}^2\begin{pmatrix}\lambda\\1\end{pmatrix}=\begin{pmatrix}s(\lambda s+c)+c(\lambda a+s)\\a(\lambda s+c)+s(\lambda a+s)\end{pmatrix}=\begin{pmatrix}\lambda(2ac+1)+2sc\\1+2a(c+\lambda s)\end{pmatrix};$$

in the same way, by $t^2=bc+1$, $\mathbf{C}^2\binom{\lambda}{1}=\binom{\lambda(2bc+1)+2tc}{1+2b(c+\lambda t)}$. The first coordinates are V_1^λ and W_1^λ.

We finally prove the monotonicity. Let $(X_j)_{j\geq 0}$ be one of the four coordinate sequences of $\mathbf{B}^{2j}\binom{\lambda}{1}$ and $\mathbf{C}^{2j}\binom{\lambda}{1}$. By the recurrences, $X_{j+1}-X_j=4acX_j+(X_j-X_{j-1})$ for $j\geq 1$ in the first two cases, and $X_{j+1}-X_j=4bcX_j+(X_j-X_{j-1})$ in the last two. Moreover $X_1>X_0$ and $X_1>0$: the second coordinates start at 1 and the first at λ, and, since $c-s=b+r>0$, $c-t=a+r>0$ and $s-a=t-b=r$ (Definition 2.3),

$$1+2a(c+\lambda s)\geq 1+2a(c-s)>1,\qquad 1+2b(c+\lambda t)\geq 1+2b(c-t)>1,$$
$$V_1^\lambda,\,W_1^\lambda\geq 2cr-1>1\geq\lambda.$$

If $X_j>0$ and $X_j>X_{j-1}$ for some $j\geq 1$, the identity above gives $X_{j+1}>X_j>0$. By induction, $(X_j)_{j\geq 0}$ is strictly increasing, and $X_j>0$ for $j\geq 1$.

□

We quote two results on the fundamental solutions of these Pell equations; they are the inputs of Proposition 2.11.

Theorem 2.9. *Let d be an extension of an Euler triple $\{a,b,c\}$ with roots r,s,t and multiplication matrices $\mathbf{B},\mathbf{C}$, and let x,y,z be as in Definition 2.5. There are integers $k_1,k_2\geq 0$ and integers z_1,x_1,z_2,y_2 with $x_1,y_2>0$ such that*

$$\begin{pmatrix}z\\x\end{pmatrix}=\mathbf{B}^{k_1}\begin{pmatrix}z_1\\x_1\end{pmatrix},\qquad\begin{pmatrix}z\\y\end{pmatrix}=\mathbf{C}^{k_2}\begin{pmatrix}z_2\\y_2\end{pmatrix},$$

and, according to the parities of (k_1,k_2):

- *even/even: $(|z_1|,x_1;|z_2|,y_2)=(1,1;1,1)$, with $z_1=z_2$;*

- *odd/even:* $(|z_1|, x_1; |z_2|, y_2) = (t, r; 1, 1)$*, with* $z_1 z_2 < 0$*;*
- *even/odd:* $(|z_1|, x_1; |z_2|, y_2) = (1, 1; s, r)$*, with* $z_1 z_2 < 0$*;*
- *odd/odd:* $(|z_1|, x_1; |z_2|, y_2) = (t, r; s, r)$*, with* $z_1 z_2 > 0$.

Proof. This is [11, Theorem 2.1], specialised to an Euler triple; that theorem completes [18, Theorem 1.3] by the values of the second coordinates. In the source the fundamental solutions are written (z_0, x_0) and (z_1, y_1) and the exponents m, n; its matrices of multiplication by β and γ are $\mathbf{B}$ and $\mathbf{C}$ (Lemma 2.4, item 5); and the values $cr - st$, $rs - at$, $rt - bs$ that occur in its four cases are all equal to 1 (Lemma 2.4, item 2). With these values the two alternatives of the even/even case coincide, and the four cases become the four cases above. □

Lemma 2.10. *Let* $P < Q$ *be positive integers with* $PQ + 1 = S^2$ *for an integer* S*, and put* $\eta_{PQ} = S + \sqrt{PQ}$*. Every solution in positive integers* (X, Y) *of* $PY^2 - QX^2 = P - Q$ *satisfies*

$$Y\sqrt{P} + X\sqrt{Q} = (Y_0\sqrt{P} + X_0\sqrt{Q})\,\eta_{PQ}^k$$

for an integer $k \geq 0$ *and an integer solution* (X_0, Y_0) *of the same equation with*

$$1 \leq X_0 \leq \sqrt{\frac{P(Q-P)}{2(S-1)}}, \qquad 1 \leq |Y_0| \leq \sqrt{\frac{(S-1)(Q-P)}{2P}}.$$

In particular $Y_0^2 < Q^2/4$.

Proof. This is [19, Lemma 8] (numbering of the arXiv version 2), going back to [13]. For the last inequality, $S^2 - 1 = PQ$ gives $(S-1)/P = Q/(S+1)$, so $Y_0^2 \leq Q(Q-P)/(2(S+1))$; since $S \geq 2$ and $Q - P < Q$, this is less than $Q^2/4$. □

Proposition 2.11. *Every extension of an Euler triple has exactly one index system.*

Proof. Existence comes from the classification of the fundamental solutions (Theorem 2.9), which gives the second and third displays of Definition 2.5, and from the bounded fundamental solutions of the Pell equation of $\{a, b\}$ (Lemma 2.10), which give the first; uniqueness follows by comparing two index systems in the three displays. For $d > d_+(a, b, c)$ existence is known [18, Introduction]; see also [10] for the three-parameter family. The proof below is valid for every extension.

Let d be an extension of the Euler triple $\{a, b, c\}$, with roots r, s, t, units α, β, γ, multiplication matrices $\mathbf{B}, \mathbf{C}$, and x, y, z as in Definition 2.5.

We first obtain the second and third displays of Definition 2.5. By Theorem 2.9 there are integers $k_1, k_2 \geq 0$ and fundamental solutions with $\binom{z}{x} = \mathbf{B}^{k_1}\binom{z_1}{x_1}$ and $\binom{z}{y} = \mathbf{C}^{k_2}\binom{z_2}{y_2}$, in one of four parity cases. Let $\varepsilon \in \{-1, 1\}$ be the sign of z_1. By the one-step identities of Lemma 2.4, item 6, the four cases convert as follows.

- Even/even, $k_1 = 2m_0$, $k_2 = 2n_0$: $(z_1, x_1) = (z_2, y_2) = (\varepsilon, 1)$. Take $\lambda = \varepsilon$, $m = m_0$, $n = n_0$.
- Odd/odd, $k_1 = 2m_0 + 1$, $k_2 = 2n_0 + 1$: $(z_1, x_1) = (\varepsilon t, r)$, $(z_2, y_2) = (\varepsilon s, r)$. If $\varepsilon = 1$, then $\binom{t}{r} = \mathbf{B}\binom{-1}{1}$ and $\binom{s}{r} = \mathbf{C}\binom{-1}{1}$ give $\binom{z}{x} = \mathbf{B}^{2m_0+2}\binom{-1}{1}$, $\binom{z}{y} = \mathbf{C}^{2n_0+2}\binom{-1}{1}$: take $\lambda = -1$, $m = m_0 + 1$, $n = n_0 + 1$. If $\varepsilon = -1$, then $\binom{-t}{r} = \mathbf{B}^{-1}\binom{1}{1}$ and $\binom{-s}{r} = \mathbf{C}^{-1}\binom{1}{1}$ give $\binom{z}{x} = \mathbf{B}^{2m_0}\binom{1}{1}$, $\binom{z}{y} = \mathbf{C}^{2n_0}\binom{1}{1}$: take $\lambda = 1$, $m = m_0$, $n = n_0$.
- Even/odd, $k_1 = 2m_0$, $k_2 = 2n_0 + 1$: $(z_1, x_1) = (\varepsilon, 1)$, $(z_2, y_2) = (-\varepsilon s, r)$. If $\varepsilon = 1$: $\lambda = 1$, $m = m_0$, $n = n_0$. If $\varepsilon = -1$: $\lambda = -1$, $m = m_0$, $n = n_0 + 1$.

- Odd/even, $k_1 = 2m_0+1$, $k_2 = 2n_0$: $(z_1,x_1) = (\varepsilon t, r)$, $(z_2,y_2) = (-\varepsilon, 1)$. If $\varepsilon = 1$: $\lambda = -1$, $m = m_0+1$, $n = n_0$. If $\varepsilon = -1$: $\lambda = 1$, $m = m_0$, $n = n_0$.

In every case $\binom{z}{x} = \mathbf{B}^{2m}\binom{\lambda}{1}$ and $\binom{z}{y} = \mathbf{C}^{2n}\binom{\lambda}{1}$ with the same λ and $m, n \geq 0$, which by item 2 of Lemma 2.8 are the second and third displays.

We next obtain the first display. The positive integers x, y satisfy $ay^2 - bx^2 = a(bd+1) - b(ad+1) = a - b$. By Lemma 2.10 with $(P,Q,S) = (a,b,r)$, so that $\eta_{PQ} = \alpha$, there are an integer $k \geq 0$ and integers $X_0 \geq 1$, Y_0 with $aY_0^2 - bX_0^2 = a - b$, $Y_0^2 < b^2/4$ and

$$y\sqrt{a} + x\sqrt{b} = (Y_0\sqrt{a} + X_0\sqrt{b})\,\alpha^k.$$

Write $\alpha^k = p_k + q_k\sqrt{ab}$. Then $y = Y_0 p_k + bX_0 q_k$, and in the binomial expansion of $(r+\sqrt{ab})^k$ every term of p_k except r^k contains a positive power of ab; so $y \equiv Y_0 r^k \pmod b$. On the other hand, writing $\gamma^{2n} = u + v\sqrt{bc}$, the third display gives $y = u + \lambda bv$, and in the same way $u \equiv t^{2n} = (bc+1)^n \equiv 1 \pmod b$. Hence $Y_0 r^k \equiv 1 \pmod b$, and since $r^2 = ab+1 \equiv 1 \pmod b$ (multiply by r when k is odd),

$$Y_0 \equiv 1 \pmod b \ \ (k \text{ even}), \qquad Y_0 \equiv r \pmod b \ \ (k \text{ odd}).$$

By Lemma 2.4, item 4, $b \geq 3$ and $1 \leq r < b$; and the integers in $(-\frac{b}{2}, \frac{b}{2})$ are pairwise incongruent modulo b.

If k is even, $Y_0 = 1$, hence $bX_0^2 = b$ and $X_0 = 1$; take $l = k/2$.

If k is odd, $Y_0 \in \{r, r-b\}$. The value $Y_0 = r$ gives $bX_0^2 = ar^2 - a + b = b(a^2+1)$, impossible since $a^2 < a^2+1 < (a+1)^2$. So $Y_0 = r-b$, and $bX_0^2 = a(r-b)^2 - a + b = b(r-a)^2$ by $ab+1 = r^2$; as $r > a$, $X_0 = r-a$. Then

$$Y_0\sqrt{a} + X_0\sqrt{b} = (r-b)\sqrt{a} + (r-a)\sqrt{b} = (\sqrt{a}+\sqrt{b})(r-\sqrt{ab}) = (\sqrt{a}+\sqrt{b})\,\alpha^{-1},$$

so the first display holds with $l = (k-1)/2 \geq 0$.

We finally prove uniqueness. Let $(\lambda_1, l_1, m_1, n_1)$ and $(\lambda_2, l_2, m_2, n_2)$ be index systems of d; we show first that $\lambda_1 = \lambda_2$. By the second display, $(\lambda_1\sqrt{a} + \sqrt{c})\beta^{2m_1} = (\lambda_2\sqrt{a} + \sqrt{c})\beta^{2m_2}$. If $\lambda_1 \neq \lambda_2$ then, up to exchanging the two systems, $\lambda_1 = 1$, $\lambda_2 = -1$, and

$$\beta^{2(m_2-m_1)} = \frac{\sqrt{c}+\sqrt{a}}{\sqrt{c}-\sqrt{a}} = \frac{c+a}{c-a} + \frac{2}{c-a}\sqrt{ac}.$$

The left side lies in $\mathbb{Z}[\sqrt{ac}]$, because $\beta^{\pm 1} = s \pm \sqrt{ac}$ (Lemma 2.4, item 5), and $\sqrt{ac}$ is irrational; so $(c-a) \mid 2$. But $c > 4a$ (Lemma 2.4, item 4), so $c - a > 3a \geq 3$, a contradiction.

With $\lambda_1 = \lambda_2$, after cancelling the factors $\lambda_1\sqrt{a} + \sqrt{c}$, $\lambda_1\sqrt{b} + \sqrt{c}$ and $\sqrt{a} + \sqrt{b}$, which are nonzero as $a < b < c$, the second display gives $\beta^{2(m_1-m_2)} = 1$, so $m_1 = m_2$ because $\beta > 1$. The third display gives $\gamma^{2(n_1-n_2)} = 1$, so $n_1 = n_2$, and the first gives $\alpha^{2(l_1-l_2)} = 1$, so $l_1 = l_2$.

□

We next identify the index system of the regular extension. It is used to exclude small indices in Lemma 2.14, and its common term $V_1^{-1} = W_1^{-1}$ reappears in the finite computations of Section 8 and Appendix A.

Lemma 2.12. *Let $\{a,b,c\}$ be an Euler triple. Then $d_+(a,b,c)$ is an extension of $\{a,b,c\}$, and its index system is $(-1,1,1,1)$. In particular $V_1^{-1} = W_1^{-1}$, and this common term is the number z of $d_+(a,b,c)$.*

Proof. Let r, s, t be the roots of $\{a, b, c\}$ and $d = d_+(a, b, c)$. By Lemma 2.4, item 2, $d = 4rst$ and $st = cr - 1$, so $d = 4r(cr - 1) > c$, as $r > a \geq 1$ (item 4 of Lemma 2.4). By Definition 2.3 and items 2 and 6 of Lemma 2.4 ($rs - at = rt - bs = 1$, $\mathbf{B}\binom{-1}{1} = \binom{t}{r}$, $\mathbf{C}\binom{-1}{1} = \binom{s}{r}$),

$$\mathbf{A}^2\begin{pmatrix}1\\1\end{pmatrix} = \mathbf{A}\begin{pmatrix}t\\s\end{pmatrix} = \begin{pmatrix}1+2bs\\1+2at\end{pmatrix}, \qquad \mathbf{B}^2\begin{pmatrix}-1\\1\end{pmatrix} = \mathbf{B}\begin{pmatrix}t\\r\end{pmatrix} = \begin{pmatrix}cr+st\\1+2at\end{pmatrix},$$
$$\mathbf{C}^2\begin{pmatrix}-1\\1\end{pmatrix} = \mathbf{C}\begin{pmatrix}s\\r\end{pmatrix} = \begin{pmatrix}cr+st\\1+2bs\end{pmatrix}.$$

Put $x = 1 + 2at$, $y = 1 + 2bs$ and $z = cr + st$. Since $rs = 1 + at$, $rt = 1 + bs$ and $cr - st = 1$,

$$x^2 = 1 + 4at\,rs = ad + 1, \qquad y^2 = 1 + 4bs\,rt = bd + 1, \qquad z^2 = (cr - st)^2 + 4crst = cd + 1,$$

so, by item 1 of Lemma 2.4, d is an extension of $\{a, b, c\}$ and x, y, z are its numbers of Definition 2.5. By item 2 of Lemma 2.8, the three identities above are the three displays of Definition 2.5 for $(\lambda, l, m, n) = (-1, 1, 1, 1)$, which by Proposition 2.11 is therefore the index system of d. Finally $z = V_1^{-1} = W_1^{-1}$ by Convention 2.6.

□

2.3 The index ordering and the two linear forms

For an irregular extension the indices are ordered, $3 \leq n < m < l < 2n$, and the triple is not small, $b > 4000$; the second fact is a result of Cipu, Filipin and Fujita [8], which we quote.

Theorem 2.13. *Let $\{a, b, c\}$ be a Diophantine triple with $a < b < c$, and let d be an extension of $\{a, b, c\}$ with $d > d_+(a, b, c)$. Then $b > 4000$.*

Proof. This is a result of Cipu, Filipin and Fujita [8], in the form quoted in [18, Lemma 2.1]: if $a < b < c < d_+(a, b, c) < d$, then $b > 21000$ when $b < 2a$, $b > 130000$ when $2a \leq b \leq 12a$, and $b > 4000$ when $b > 12a$. The hypothesis $c < d_+(a, b, c)$ holds because $d_+(a, b, c) > (2ab + 1)c$ (Definition 2.2). □

Lemma 2.14. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$. Then*

$$3 \leq n < m < l < 2n, \qquad m \geq 4, \qquad l \geq 5,$$

and $d > d_+(a, b, c)$ and $b > 4000$.

Proof. Each of the inequalities $n < m$, $m < l$ and $l < 2n$ compares the same coordinate, z, x or y, along two sequences built from the three displays of Definition 2.5. The two sequences satisfy second-order recurrences with different coefficients; the one with the larger coefficient stays ahead (the comparison principle below), so it reaches the common value at the smaller index.

We first set up the sequences. By items 1 and 5 of Lemma 2.4, $s^2 = ac + 1$, $t^2 = bc + 1$, and multiplication by α, β, γ acts on coordinates through $\mathbf{A}, \mathbf{B}, \mathbf{C}$. For $k \geq 0$ write $\mathbf{A}^k\binom{1}{1} = \binom{u_k}{v_k}$, i.e. $(\sqrt{a} + \sqrt{b})\alpha^k = u_k\sqrt{a} + v_k\sqrt{b}$; then $u_0 = v_0 = 1$, $u_{k+1} = ru_k + bv_k$, $v_{k+1} = au_k + rv_k$, so u_k, v_k are positive and strictly increasing in k. For $j \geq 0$ write

$$\mathbf{B}^{2j}\begin{pmatrix}\lambda\\1\end{pmatrix} = \begin{pmatrix}V_j^\lambda\\\xi_j\end{pmatrix}, \qquad \mathbf{C}^{2j}\begin{pmatrix}\lambda\\1\end{pmatrix} = \begin{pmatrix}W_j^\lambda\\\psi_j\end{pmatrix},$$

with the Pell sequences V_j^λ, W_j^λ of Convention 2.6. By item 2 of Lemma 2.8, the three displays say

$$x = v_{2l} = \xi_m, \qquad y = u_{2l} = \psi_n, \qquad z = V_m^\lambda = W_n^\lambda.$$

By item 3 of Lemma 2.8, the sequences $(v_{2j})_j$, $(V_j^\lambda)_j$ and $(\xi_j)_j$, $(W_j^\lambda)_j$ and $(\psi_j)_j$ satisfy $X_{j+1} = TX_j - X_{j-1}$ $(j \geq 1)$ with $T = 4ab+2$, $4ac+2$, $4bc+2$ respectively; and $(u_{4j})_j$ satisfies it with $T = T_\alpha := \alpha^4 + \alpha^{-4} = 2(8r^4 - 8r^2 + 1)$, since α^4 and α^{-4} are the roots of $X^2 - T_\alpha X + 1$. The initial values of (V_j^λ) and (W_j^λ) are given in item 3 of Lemma 2.8; those of the other sequences are $v_0 = \xi_0 = \psi_0 = u_0 = 1$ and

$$v_2 = 1 + 2a(b+r), \qquad \xi_1 = 1 + 2a(c+\lambda s),$$

$$\psi_1 = 1 + 2b(c+\lambda t), \qquad u_4 = 8r^4 - 8r^2 + 1 + 4br(2r^2-1).$$

We use the following comparison principle. Let $X_{j+1} = T_1X_j - X_{j-1}$ and $Y_{j+1} = T_2Y_j - Y_{j-1}$ $(j \geq 1)$ with $T_1 > T_2 \geq 2$, and let $j_0 \geq 1$ be such that $\delta_j = X_j - Y_j$ satisfies $\delta_{j_0} > \delta_{j_0-1} \geq 0$ and $X_j > 0$ for $j \geq j_0$. Then $X_j > Y_j$ for all $j \geq j_0$. Indeed $\delta_{j+1} - \delta_j = (T_2-2)\delta_j + (\delta_j - \delta_{j-1}) + (T_1 - T_2)X_j$, so by induction $\delta_{j+1} > \delta_j > 0$ for $j \geq j_0$. By item 3 of Lemma 2.8, the sequences (ξ_j), (V_j^λ), (W_j^λ), (ψ_j) are strictly increasing and positive for $j \geq 1$.

We next exclude small indices. If $m = 0$ or $n = 0$ then $z = \lambda$ and $cd = z^2 - 1 = 0$, impossible. By Lemma 2.12, $V_1^{-1} = W_1^{-1}$ is the number z_+ of the regular extension. If $\lambda = -1$ and $m = 1$ or $n = 1$, then $z = z_+$, so $d = (z^2-1)/c = d_+(a,b,c)$, contradicting irregularity. Hence $m, n \geq 1$, and $m, n \geq 2$ when $\lambda = -1$. Put $j_0 = 1$ if $\lambda = 1$ and $j_0 = 2$ if $\lambda = -1$; then $m, n \geq j_0$.

We next prove $m > n$. Here $W_1^\lambda - V_1^\lambda = 2c(b-a)(1+\lambda)$ because $t - s = b - a$. If $\lambda = 1$, $W_1^\lambda - V_1^\lambda = 4c(b-a) > 0 = W_0^\lambda - V_0^\lambda$. If $\lambda = -1$, $W_1^\lambda = V_1^\lambda$ and $W_2^\lambda - V_2^\lambda = 4(b-a)cW_1^\lambda > 0$. The comparison principle with $T_1 = 4bc+2 > T_2 = 4ac+2$ gives $W_j^\lambda > V_j^\lambda$ for $j \geq j_0$, in particular $W_n^\lambda > V_n^\lambda$. If $m \leq n$, then $z = V_m^\lambda \leq V_n^\lambda < W_n^\lambda = z$, since (V_j^λ) is increasing. So $m > n$.

We next prove $l > m$. Here $\xi_1 - v_2 = 2a(c + \lambda s - b - r) = 2as(1+\lambda)$. If $\lambda = 1$ this is positive; if $\lambda = -1$, $\xi_1 = v_2$ and $\xi_2 - v_4 = 4a(c-b)v_2 > 0$. The comparison principle with $T_1 = 4ac+2 > T_2 = 4ab+2$ gives $\xi_j > v_{2j}$ for $j \geq j_0$, in particular $\xi_m > v_{2m}$. If $l \leq m$, then $x = v_{2l} \leq v_{2m} < \xi_m = x$. So $l > m$.

We next prove $l < 2n$. First $T_\alpha > 4bc+2$: this is $16r^2(r^2-1) > 4bc$, i.e. $4ar^2 > c$, true as $4ar^2 > 4b > a + b + 2r = c$ (by $a < r < b$, Lemma 2.4, item 4). Second $u_4 > \psi_1$: since $\psi_1 \leq 1 + 2b(c+t) = 1 + 2b(a + 2b + 3r)$,

$$u_4 - \psi_1 \geq 8r^2(r^2-1) + 2b\big(r(4r^2-5) - a - 2b\big) > 0,$$

because $r(4r^2-5) = r(4ab-1) \geq 2(4b-1) > a + 2b$. With $u_0 = \psi_0$, the comparison principle with $T_1 = T_\alpha > T_2 = 4bc+2$ and $j_0 = 1$ gives $u_{4j} > \psi_j$ for $j \geq 1$. If $l \geq 2n$, then $y = u_{2l} \geq u_{4n} > \psi_n = y$. So $l < 2n$.

Next, $n < m < l < 2n$ places two distinct integers strictly between n and $2n$, so $n \geq 3$, $m \geq n+1 \geq 4$ and $l \geq m+1 \geq 5$.

We finally prove $d > d_+(a,b,c)$ and $b > 4000$. Since (V_j^λ) is increasing, $m \geq 2$ and $V_1^1 - V_1^{-1} = 2(2ac+1) > 0$, we have $z = V_m^\lambda > V_1^\lambda \geq V_1^{-1} = z_+$. Hence $d = (z^2-1)/c > (z_+^2-1)/c = d_+(a,b,c)$. By Theorem 2.13, applied to the Diophantine triple $\{a,b,c\}$ (Lemma 2.4, item 1), $b > 4000$.

□

We now turn to the two linear forms. Each of x and z is a coordinate of two of the three representations, and the closed forms below write it in two ways.

Lemma 2.15. *Let (λ, l, m, n) be an index system of an extension d of an Euler triple $\{a, b, c\}$ with units α, β, γ, and let x, y, z be as in Definition 2.5. Then*

$$2x = \Big(1 + \sqrt{\tfrac{a}{b}}\Big)\alpha^{2l} + \Big(1 - \sqrt{\tfrac{a}{b}}\Big)\alpha^{-2l} = \Big(1 + \lambda\sqrt{\tfrac{a}{c}}\Big)\beta^{2m} + \Big(1 - \lambda\sqrt{\tfrac{a}{c}}\Big)\beta^{-2m},$$

$$2z = \Big(\sqrt{\tfrac{c}{a}} + \lambda\Big)\beta^{2m} + \Big(\lambda - \sqrt{\tfrac{c}{a}}\Big)\beta^{-2m} = \Big(\sqrt{\tfrac{c}{b}} + \lambda\Big)\gamma^{2n} + \Big(\lambda - \sqrt{\tfrac{c}{b}}\Big)\gamma^{-2n}.$$

Proof. By Lemma 2.4, item 5, $(u\sqrt{a} + v\sqrt{b})\alpha = u_1\sqrt{a} + v_1\sqrt{b}$ with $\binom{u_1}{v_1} = \mathbf{A}\binom{u}{v}$ for integers u, v; since $\alpha^{-1} = r - \sqrt{ab}$, the same expansion gives $(u\sqrt{a} - v\sqrt{b})\alpha^{-1} = u_1\sqrt{a} - v_1\sqrt{b}$. By induction on $k \geq 0$, for integers u_0, v_0 the identity $(u_0\sqrt{a} + v_0\sqrt{b})\alpha^k = u\sqrt{a} + v\sqrt{b}$ implies $(u_0\sqrt{a} - v_0\sqrt{b})\alpha^{-k} = u\sqrt{a} - v\sqrt{b}$, the coordinates being unique because ab is not a square. The same holds for β with $\sqrt{a}, \sqrt{c}$ and $\mathbf{B}$, and for γ with $\sqrt{b}, \sqrt{c}$ and $\mathbf{C}$. So the three displays of Definition 2.5 imply

$$y\sqrt{a} - x\sqrt{b} = (\sqrt{a} - \sqrt{b})\alpha^{-2l}, \qquad z\sqrt{a} - x\sqrt{c} = (\lambda\sqrt{a} - \sqrt{c})\beta^{-2m},$$
$$z\sqrt{b} - y\sqrt{c} = (\lambda\sqrt{b} - \sqrt{c})\gamma^{-2n}.$$

Subtracting the first two of these identities from the corresponding displays and dividing by $\sqrt{b}$ and by $\sqrt{c}$ gives the two expressions of $2x$; adding the last two to the corresponding displays and dividing by $\sqrt{a}$ and by $\sqrt{b}$ gives the two expressions of $2z$.

□

Definition 2.16. Let $\{a, b, c\}$ be an Euler triple with units α, β, γ (Definition 2.3). For $\lambda \in \{-1, 1\}$ put

$$D_\lambda = \frac{\sqrt{bc} + \sqrt{ac}}{\sqrt{bc} + \lambda\sqrt{ab}}, \qquad E_\lambda = \frac{\sqrt{bc} + \lambda\sqrt{ab}}{\sqrt{ac} + \lambda\sqrt{ab}}, \qquad \kappa_\lambda = \frac{2c(b-a)}{b(\sqrt{c} + \lambda\sqrt{a})^2}.$$

The **linear forms** of an index system (λ, l, m, n) (Definition 2.5) of an extension of $\{a, b, c\}$ are

$$\Lambda_x = 2l\log\alpha - 2m\log\beta + \log D_\lambda, \qquad \Lambda_z = 2m\log\beta - 2n\log\gamma + \log E_\lambda,$$

and the **gap ratios** of $\{a, b, c\}$ are

$$R_x = \sqrt{\frac{b}{a}}\,\log\alpha, \qquad R_z = \frac{\sqrt{ac}}{b-a}\,\log\beta.$$

The numbers D_λ and E_λ are the ratios of the leading coefficients of the two expressions of x and of z in Lemma 2.15, so that Λ_x and Λ_z are the logarithms of the ratios of the leading terms. The number κ_λ is the constant of the bound $\Lambda_z < \kappa_\lambda\beta^{-4m}$ of Lemma 2.18, item 5, which is the form in which the reduction of Appendix B uses Λ_z; the gap ratios are the factors of the gap inequalities, item 3 there. The two comparisons are one argument, which we prove once, for two abstract expressions; it is the one technical step of this section.

Lemma 2.17. *Let $\mu_1 > \mu_2 > 0$, ν_1 and ν_2 be real numbers with $\nu_1 < \mu_2$ and $\mu_1 + \nu_1 = \mu_2 + \nu_2$, and put $e_i = \mu_i\nu_i$ for $i = 1, 2$. Let $u_1 \geq 1$ and $u_2 > 1$ be real numbers with*

$$\mu_1 u_1 + \nu_1 u_1^{-1} = \mu_2 u_2 + \nu_2 u_2^{-1},$$

and put $X_i = \mu_i u_i$. Then $e_1 < e_2$ and $X_2^2 > e_2$, and:

1. $u_1 < u_2$ *and* $X_1 > X_2$, *that is,* $0 < \log(X_1/X_2) < \log(\mu_1/\mu_2)$;

2. $\log(X_1/X_2) < \dfrac{e_2 - e_1}{X_2^2 - e_2}$;

3. *if* $e_2 \le 0$ *and* $2(e_2 - e_1) \le X_1^2$, *then* $\log(X_1/X_2) < \dfrac{2(e_2 - e_1)}{X_1^2}$.

Proof. We compare the two expressions, which agree at $u_1 = u_2 = 1$, in three ways: at equal arguments the first is the larger, which gives the upper side of item 1; at equal leading terms it is the smaller, which gives the lower side; and one exact identity between the leading terms gives the size of $\log(X_1/X_2)$, items 2 and 3.

Put $\sigma = \mu_1 + \nu_1 = \mu_2 + \nu_2$, and, for $i = 1, 2$, a real number e and real numbers $u, X > 0$,

$$F_i(u) = \mu_i u + \nu_i u^{-1}, \qquad h_e(X) = X + eX^{-1}.$$

Then $F_i(u) = h_{e_i}(\mu_i u)$, because $e_i(\mu_i u)^{-1} = \nu_i u^{-1}$; moreover $F_1(1) = F_2(1) = \sigma$, and the hypothesis reads $F_1(u_1) = F_2(u_2)$, that is, $h_{e_1}(X_1) = h_{e_2}(X_2)$. Since $\mu_1, \mu_2 > 0$ and $u_1, u_2 \ge 1$, we have $X_1, X_2 > 0$.

We first prove $e_1 < e_2$. Since $\nu_i = \sigma - \mu_i$, one has $e_i = \sigma\mu_i - \mu_i^2$, so

$$e_2 - e_1 = (\mu_1^2 - \mu_2^2) - \sigma(\mu_1 - \mu_2) = (\mu_1 - \mu_2)(\mu_1 + \mu_2 - \sigma) = (\mu_1 - \mu_2)(\mu_2 - \nu_1),$$

and both factors are positive, as $\mu_1 > \mu_2$ and $\nu_1 < \mu_2$.

We next prove $u_1 < u_2$. Since $\nu_1 - \nu_2 = \mu_2 - \mu_1$,

$$F_1(u) - F_2(u) = (\mu_1 - \mu_2)(u - u^{-1}) > 0 \qquad (u > 1).$$

For $u \ge 1$ one has $\nu_1 u^{-2} \le \max\{\nu_1, 0\} < \mu_1$, because $\nu_1 < \mu_2 < \mu_1$; hence $F_1'(u) = \mu_1 - \nu_1 u^{-2} > 0$, and F_1 is strictly increasing on $[1, \infty)$. If $u_1 \ge u_2$, then, as $u_2 > 1$, $F_1(u_1) \ge F_1(u_2) > F_2(u_2)$, which contradicts $F_1(u_1) = F_2(u_2)$. So $u_1 < u_2$.

We next prove $X_2^2 > e_2$. Suppose that $X_2^2 \le e_2$. Then $e_2 > 0$, so $\nu_2 > 0$; and $u_2^2 \le \nu_2/\mu_2$, because $X_2^2 = \mu_2^2 u_2^2$ and $e_2 = \mu_2\nu_2$. Thus $1 < u_2 \le (\nu_2/\mu_2)^{1/2}$. For $0 < u < (\nu_2/\mu_2)^{1/2}$ one has $F_2'(u) = \mu_2 - \nu_2 u^{-2} < 0$, so F_2 is strictly decreasing on $(0, (\nu_2/\mu_2)^{1/2}]$, and $F_2(u_2) < F_2(1) = \sigma$. On the other hand $F_1(u_1) \ge F_1(1) = \sigma$, because $u_1 \ge 1$ and F_1 is increasing on $[1, \infty)$. Hence $F_2(u_2) < F_1(u_1)$, a contradiction.

We next prove $X_1 > X_2$. For $X > 0$ one has $h_e'(X) = 1 - eX^{-2}$. Since $u_1 \ge 1$ and $\mu_1 > \nu_1$, $X_1^2 \ge \mu_1^2 > \mu_1\nu_1 = e_1$; so $h_{e_1}'(X) > 0$ for $X \ge X_1$, and h_{e_1} is strictly increasing on $[X_1, \infty)$. If $X_1 \le X_2$, then

$$h_{e_1}(X_1) \le h_{e_1}(X_2) < h_{e_2}(X_2),$$

the second inequality because $e_1 < e_2$ and $X_2 > 0$; this contradicts $h_{e_1}(X_1) = h_{e_2}(X_2)$. So $X_1 > X_2$. Since $\log(X_1/X_2) = \log(\mu_1/\mu_2) + \log(u_1/u_2)$, the inequalities $u_1 < u_2$ and $X_1 > X_2$ say that $0 < \log(X_1/X_2) < \log(\mu_1/\mu_2)$, which is item 1.

We next derive the exact identity on which items 2 and 3 rest. The relation $h_{e_1}(X_1) = h_{e_2}(X_2)$ reads $X_1 - X_2 = e_2 X_2^{-1} - e_1 X_1^{-1}$. Multiplying by X_1X_2 gives $(X_1 - X_2)X_1X_2 = e_2X_1 - e_1X_2$, and subtracting $e_2(X_1 - X_2)$ from both sides gives

$$(X_1 - X_2)(X_1X_2 - e_2) = (e_2 - e_1)X_2.$$

We next prove item 2. Since $X_1 > X_2 > 0$ and $X_2^2 > e_2$, we have $X_1X_2 - e_2 > X_2^2 - e_2 > 0$. Since $X_1/X_2 > 1$ and the logarithm lies strictly below its tangent line at 1, the identity gives

$$\log \frac{X_1}{X_2} < \frac{X_1 - X_2}{X_2} = \frac{e_2 - e_1}{X_1X_2 - e_2} < \frac{e_2 - e_1}{X_2^2 - e_2},$$

the last step because $e_2 - e_1 > 0$.

We finally prove item 3. Let $e_2 \le 0$ and $2(e_2 - e_1) \le X_1^2$. Since $0 < X_2 < X_1$ and $e_2 \le 0$, we have $e_2X_2^{-1} \le e_2X_1^{-1}$, so

$$X_1 - X_2 = e_2X_2^{-1} - e_1X_1^{-1} \le (e_2 - e_1)X_1^{-1}.$$

Hence $\delta = 1 - X_2/X_1$ satisfies $0 < \delta \le (e_2 - e_1)/X_1^2 \le \frac{1}{2}$. For $0 < \delta < 1$ one has $-\log(1-\delta) = \sum_{k\ge1} \delta^k/k < \sum_{k\ge1} \delta^k = \delta/(1-\delta)$, and $\delta/(1-\delta) \le 2\delta$ because $\delta \le \frac{1}{2}$. Therefore

$$\log \frac{X_1}{X_2} = -\log(1-\delta) < \frac{\delta}{1-\delta} \le 2\delta \le \frac{2(e_2 - e_1)}{X_1^2}.$$

□

Lemma 2.18. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$, with the linear forms, the gap ratios and the numbers $D_\lambda, E_\lambda, \kappa_\lambda$ of Definition 2.16. Then:*

1. $l \log \alpha < m \log \beta < n \log \gamma$;
2. $\sqrt{a/c} < \log(\beta/\alpha) < \sqrt{a/b}$, $\dfrac{b-a}{\sqrt{bc}} < \log(\gamma/\beta) < \dfrac{b-a}{\sqrt{ac}}$, *and* $\log(\gamma/\alpha) < \sqrt{b/a}$;
3. $m > (l-m)R_x$ *and* $n > (m-n)R_z$;
4. $0 < \Lambda_x < \min\{\log D_\lambda,\ 4.01\,\beta^{-4m}\}$;
5. $0 < \Lambda_z < \min\{\log E_\lambda,\ \kappa_\lambda\beta^{-4m},\ 2\beta^{-4n}\}$.

Proof. Items 1, 4 and 5 compare the two expressions of x and of z given by Lemma 2.15, by Lemma 2.17; items 2 and 3 are elementary. By Lemma 2.14, $3 \le n < m < l < 2n$ and $m \ge 4$. By items 1 and 4 of Lemma 2.4, $s^2 = ac + 1$, $t^2 = bc + 1$ and $c > 4a$; so $\sqrt{a/c} < \frac{1}{2}$, and $\beta = s + \sqrt{ac} > 2\sqrt{ac}$.

We first compare the two expressions of x. By Lemma 2.15, $2x = \mu_1u_1 + \nu_1u_1^{-1} = \mu_2u_2 + \nu_2u_2^{-1}$ with

$$(\mu_1, \nu_1, u_1) = \big(1 + \sqrt{a/b},\ 1 - \sqrt{a/b},\ \alpha^{2l}\big), \qquad (\mu_2, \nu_2, u_2) = \big(1 + \lambda\sqrt{a/c},\ 1 - \lambda\sqrt{a/c},\ \beta^{2m}\big).$$

The hypotheses of Lemma 2.17 hold: $\mu_1 + \nu_1 = \mu_2 + \nu_2 = 2$; $\mu_1 > \mu_2 \ge 1 - \sqrt{a/c} > \frac{1}{2}$ and $\nu_1 < \mu_2$, because $\sqrt{a/c} < \sqrt{a/b}$; and $u_1 \ge 1$, $u_2 > 1$. Dividing the numerator and the denominator of D_λ by $\sqrt{bc}$ gives $\mu_1/\mu_2 = D_\lambda$, so $\log(\mu_1u_1/(\mu_2u_2)) = \Lambda_x$. Item 1 of Lemma 2.17 gives $\alpha^{2l} < \beta^{2m}$ and $0 < \Lambda_x < \log D_\lambda$. Here $e_1 = 1 - a/b$ and $e_2 = 1 - a/c$, so $0 < e_2 - e_1 < 1$ and $e_2 < 1$; with $\mu_2u_2 > \frac{1}{2}\beta^{2m}$, item 2 gives

$$\Lambda_x < \frac{1}{\frac{1}{4}\beta^{4m} - 1} = \frac{4}{\beta^{4m} - 4} < 4.01\,\beta^{-4m},$$

the last inequality because $\beta^{4m} \geq \beta^{16} > (4ac)^8 > 1604$.

We next compare the two expressions of z. By Lemma 2.15, $2z = \mu_1 u_1 + \nu_1 u_1^{-1} = \mu_2 u_2 + \nu_2 u_2^{-1}$ with

$$(\mu_1, \nu_1, u_1) = \big(\sqrt{c/a} + \lambda,\ \lambda - \sqrt{c/a},\ \beta^{2m}\big), \qquad (\mu_2, \nu_2, u_2) = \big(\sqrt{c/b} + \lambda,\ \lambda - \sqrt{c/b},\ \gamma^{2n}\big).$$

The hypotheses hold: $\mu_1 + \nu_1 = \mu_2 + \nu_2 = 2\lambda$; $\mu_1 > \mu_2 > 0$ and $\nu_1 < 0 < \mu_2$, because $a < b < c$; and $u_1, u_2 > 1$. Here $\mu_1/\mu_2 = E_\lambda$, so $\log(\mu_1 u_1/(\mu_2 u_2)) = \Lambda_z$, and item 1 gives $\beta^{2m} < \gamma^{2n}$ and $0 < \Lambda_z < \log E_\lambda$. Here $e_1 = 1 - c/a$ and $e_2 = 1 - c/b < 0$, so $e_2 - e_1 = c(b-a)/(ab)$ and $2(e_2 - e_1)/(\mu_1 u_1)^2 = \kappa_\lambda \beta^{-4m}$. Since $\sqrt{c} + \lambda\sqrt{a} \geq \sqrt{c} - \sqrt{a} > \frac{1}{2}\sqrt{c}$, we have $\kappa_\lambda < 8(b-a)/b < 8$, while $\beta^4 > 16a^2c^2 \geq 16$; so $\kappa_\lambda \beta^{-4m} < 1$, and item 3 gives $\Lambda_z < \kappa_\lambda \beta^{-4m}$. Finally $m \geq n+1$ gives $\kappa_\lambda \beta^{-4m} < 8\beta^{-4}\beta^{-4n} < 2\beta^{-4n}$.

The two comparisons give $\alpha^{2l} < \beta^{2m} < \gamma^{2n}$, which is item 1, and items 4 and 5.

We next prove item 2 by one mean-value step. As $\alpha = r + \sqrt{r^2 - 1}$, $\beta = s + \sqrt{s^2 - 1}$ and $\gamma = t + \sqrt{t^2 - 1}$, one has $\log \alpha = f(r)$, $\log \beta = f(s)$, $\log \gamma = f(t)$ for $f(u) = \log(u + \sqrt{u^2 - 1})$, whose derivative $(u^2 - 1)^{-1/2}$ is strictly decreasing on $(1, \infty)$. By the mean value theorem on $[r, s]$, $[s, t]$ and $[r, t]$, where $s - r = a$, $t - s = b - a$ and $t - r = b$,

$$\frac{a}{\sqrt{s^2-1}} < \log\frac{\beta}{\alpha} < \frac{a}{\sqrt{r^2-1}}, \qquad \frac{b-a}{\sqrt{t^2-1}} < \log\frac{\gamma}{\beta} < \frac{b-a}{\sqrt{s^2-1}}, \qquad \log\frac{\gamma}{\alpha} < \frac{b}{\sqrt{r^2-1}},$$

and $\sqrt{r^2 - 1} = \sqrt{ab}$, $\sqrt{s^2 - 1} = \sqrt{ac}$, $\sqrt{t^2 - 1} = \sqrt{bc}$ give item 2.

We next prove item 3, by an argument adapted from Cipu, Fujita and Mignotte [10]. By items 1 and 2, $(l - m)\log\alpha < m\log(\beta/\alpha) < m\sqrt{a/b}$, which is $m > (l - m)R_x$. Likewise $(m - n)\log\beta < n\log(\gamma/\beta) < n(b-a)/\sqrt{ac}$, which is $n > (m - n)R_z$. □

Items 4 and 5 are the input of every bound by linear forms in logarithms below, in Sections 4 and 7 and in Appendix B, and item 3, the gap inequalities, is the lower side of the criterion for close units. The lower bound for the index that holds for every irregular extension is the subject of the next section.

3 A quartic index floor

This section proves the quartic index floor (Theorem 3.6). The exponent 4 has a simple source: the index polynomials of the convention below are quadratic in l, m, n, the second-order congruences make the order-two quotients integers, with $0 < k_c < H$ (Lemma 3.2), and each of the two bounds of the section multiplies two quadratic quantities, k_c and L_3 in the bracket for c (Lemma 3.4), and the index polynomials and k_c in the bound for $a + b$ that the cofactor triples give (Lemma 3.5). The bracket also needs the third-order congruence modulo c of Lemma 3.3.

Convention 3.1. Let $\{a, b, c\}$ be an Euler triple with roots r, s, t (Definition 2.3), and let $\lambda \in \{-1, 1\}$ and l, m, n be integers; when (λ, l, m, n) is an index system (Definition 2.5), the quantities below are evaluated at it. The **index polynomials** are

$$L_1 = l^2 - m^2, \qquad L_2 = l^2 - n^2, \qquad L_3 = m^2 - n^2,$$

$$M_1 = 2m^2 + \lambda m - l, \qquad M_2 = 2n^2 + \lambda n - l,$$

$$H_1 = m(m + \lambda), \qquad H_2 = n(n + \lambda), \qquad H = H_1 + H_2,$$

$$B_m = 2m^2 + \lambda(m + n), \qquad B_n = 2n^2 + \lambda(m + n),$$

and the **order-two quotients** are the rational numbers

$$k_a = \frac{bL_1 - rM_1}{a}, \qquad k_b = \frac{aL_2 - rM_2}{b}, \qquad k_c = \frac{aH + rB_n}{c}.$$

Lemma 3.2. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$, with the index polynomials and the order-two quotients k_a, k_b, k_c of Convention 3.1. Then:*

1. *the index polynomials satisfy*

$$\begin{aligned}(bl^2 + rl) - (cm^2 + \lambda sm) &= bL_1 - rM_1 - aH_1,\\ (al^2 + rl) - (cn^2 + \lambda tn) &= aL_2 - rM_2 - bH_2,\\ am^2 + \lambda sm - bn^2 - \lambda tn &= aH + rB_n - cH_2;\end{aligned}$$

2. *k_a, k_b, k_c are integers, $k_a < 0$, $k_b < 0$ and $0 < k_c < H$.*

Proof. Item 1 consists of polynomial identities. Integrality comes from comparing, for each of x, y and z, the second-order congruences of the two Pell equations that contain it; the signs of k_a and k_b come from the index inequalities of Lemma 2.18, and the bounds for k_c from the index ordering. Throughout, $c = a + b + 2r$, $s = a + r$, $t = b + r$ and $r^2 = ab + 1$ (Definition 2.3), so that $ac + 1 = s^2$ and $bc + 1 = t^2$ (item 1 of Lemma 2.4), and the index polynomials are those of Convention 3.1. By Lemma 2.14, $3 \le n < m < l < 2n$, so $l \le 2n - 1 \le 2m - 3$ and $m \le 2n - 2$.

We first prove item 1. Substituting $c = a + b + 2r$, $s = a + r$ and $t = b + r$ and expanding the index polynomials, the two sides of each identity become the same polynomial in a, b, r, with λ, l, m, n as parameters.

We next prove that k_a, k_b, k_c are integers. By items 1 and 2 of Lemma 2.8, $y\sqrt{a} + x\sqrt{b}$, $z\sqrt{a} + x\sqrt{c}$ and $z\sqrt{b} + y\sqrt{c}$ are the terms of index $2l$, $2m$, $2n$ of the orbits of Lemma 2.7 with $(P, Q, S, u_0, v_0) = (a, b, r, 1, 1)$, $(a, c, s, \lambda, 1)$ and $(b, c, t, \lambda, 1)$ respectively. Item 2 of Lemma 2.7, applied to x in the first two orbits, to y in the first and the third, and to z in the last two, gives

$$x \equiv 1 + 2a(bl^2 + rl) \equiv 1 + 2a(cm^2 + \lambda sm) \pmod{8a^2},$$

$$y \equiv 1 + 2b(al^2 + rl) \equiv 1 + 2b(cn^2 + \lambda tn) \pmod{8b^2},$$

$$z \equiv \lambda + 2c(\lambda am^2 + sm) \equiv \lambda + 2c(\lambda bn^2 + tn) \pmod{8c^2}.$$

Cancelling $2a$, $2b$, $2c$ and multiplying the last congruence by λ,

$$4a \mid (bl^2 + rl) - (cm^2 + \lambda sm), \qquad 4b \mid (al^2 + rl) - (cn^2 + \lambda tn), \qquad 4c \mid am^2 + \lambda sm - bn^2 - \lambda tn.$$

By item 1, these three differences are

$$bL_1 - rM_1 - aH_1, \qquad aL_2 - rM_2 - bH_2, \qquad aH + rB_n - cH_2,$$

so $a \mid bL_1 - rM_1$, $b \mid aL_2 - rM_2$ and $c \mid aH + rB_n$, that is, $k_a, k_b, k_c \in \mathbb{Z}$.

We next bound $\log \alpha$. By Lemma 2.14, $b > 4000$, so $r^2 = ab + 1 > 4000$ and $r \ge 64$. Since $\alpha = r + \sqrt{ab} > r$,

$$\log \alpha > \log 64 > 3.$$

We next prove $k_a < 0$ and $k_b < 0$, by one argument. By item 3 of Lemma 2.18, with the gap ratio R_x of Definition 2.16, $m > (l-m)R_x = (l-m)\sqrt{b/a}\,\log\alpha$, so $(l-m)\log\alpha < m\sqrt{a/b}$; and $l+m<3m$, as $l<2n<2m$. Hence

$$bL_1 = b(l-m)(l+m) < \frac{3\sqrt{ab}}{\log\alpha}\,m^2 < rm^2 < rM_1,$$

since $\sqrt{ab}<r$, $\log\alpha>3$ and $M_1 \geq 2m^2-m-(2m-3) = 2m^2-3m+3 > m^2$; so $k_a<0$. By items 1 and 2 of Lemma 2.18, $l\log\alpha < n\log\gamma < n(\log\alpha+\sqrt{b/a})$, so $(l-n)\log\alpha < n\sqrt{b/a}$; and $l+n<3n$, as $l<2n$. Hence

$$aL_2 = a(l-n)(l+n) < \frac{3\sqrt{ab}}{\log\alpha}\,n^2 < rn^2 < rM_2,$$

since $M_2 \geq 2n^2-n-(2n-1) = 2n^2-3n+1 > n^2$, as $n\geq 3$; so $k_b<0$.

We finally prove $0<k_c<H$. Clearly $H>0$, and $B_n \geq 2n^2-(2n-2)-n = 2n^2-3n+2>0$, so $k_c>0$. Since $2H-B_n = B_m = 2m^2+\lambda(m+n)>0$, we have $aH+rB_n < (a+2r)H < cH$, so $k_c<H$.

□

Lemma 3.3. *Let (λ,l,m,n) be the index system of an irregular extension d of an Euler triple $\{a,b,c\}$, with the order-two quotient k_c and the index polynomial H_2 of Convention 3.1, and put*

$$A_z = a(m^3-m)(2s+\lambda am) - b(n^3-n)(2t+\lambda bn).$$

Then $A_z + 3\lambda(k_c-H_2) \equiv 0 \pmod{24c}$.

Proof. Following [20], we expand the common term z to third order along each of the two Pell equations that contain it, modulo $16c^3$, and compare. By item 2 of Lemma 3.2, k_c is an integer. For $q\geq 0$ put

$$f_a(q) = \lambda + 2c(\lambda a q^2 + sq) + \tfrac{2}{3}ac^2(q^3-q)(2s+\lambda aq),$$

an integer since $6 \mid q^3-q$, and define $f_b(q)$ in the same way with (b,t) in place of (a,s).

We first prove $V_q^\lambda \equiv f_a(q)$ and $W_q^\lambda \equiv f_b(q) \pmod{16c^3}$ for all $q\geq 0$, with the Pell sequences of Convention 2.6. One has $f_a(0) = \lambda = V_0^\lambda$ and $f_a(1) = \lambda(2ac+1)+2sc = V_1^\lambda$, by item 3 of Lemma 2.8. Identically in a,c,s,

$$f_a(q+2) - (4ac+2)f_a(q+1) + f_a(q) = -\tfrac{8}{3}a^2c^3\,q(q+1)(q+2)\big(2s+\lambda a(q+1)\big) \equiv 0 \pmod{16c^3},$$

because $6 \mid q(q+1)(q+2)$. By item 3 of Lemma 2.8, the sequence $(V_q^\lambda)_q$ satisfies $V_{q+2}^\lambda = (4ac+2)V_{q+1}^\lambda - V_q^\lambda$. Induction on q gives $V_q^\lambda \equiv f_a(q) \pmod{16c^3}$. The same argument with (b,t) in place of (a,s) gives $W_q^\lambda \equiv f_b(q) \pmod{16c^3}$.

We next compare the two expansions at the common term. By item 2 of Lemma 2.8, $z = V_m^\lambda = W_n^\lambda$. By item 1 of Lemma 3.2, $aH+rB_n-cH_2 = am^2+\lambda sm-bn^2-\lambda tn$, and $aH+rB_n = ck_c$; hence $\lambda(am^2-bn^2)+sm-tn = \lambda c(k_c-H_2)$. Therefore

$$\begin{aligned} 0 = V_m^\lambda - W_n^\lambda \equiv f_a(m) - f_b(n) &= 2c\big(\lambda(am^2-bn^2)+sm-tn\big) + \tfrac{2}{3}c^2A_z \\ &= \tfrac{2}{3}c^2\big(A_z + 3\lambda(k_c-H_2)\big) \pmod{16c^3}. \end{aligned}$$

Since 6 divides m^3-m and n^3-n, $3 \mid A_z$, and dividing by $2c^2$ gives $A_z/3 + \lambda(k_c-H_2) \equiv 0 \pmod{8c}$, that is $A_z + 3\lambda(k_c-H_2) \equiv 0 \pmod{24c}$.

□

The bracket below is the main step. Its lower end $\Psi(m,n)$ is shown to be positive when $m \le \frac{3}{2}n$, and the end of its proof shows by two examples that this condition cannot be replaced by $m < 2n$; the range $m > \frac{3}{2}n$ is covered by the bound for $a+b$ that follows it, since $c \le 2(a+b)$ (Lemma 2.4).

Lemma 3.4. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a,b,c\}$, with the index polynomials and the order-two quotient k_c of Convention 3.1. Put*

$$\Psi(u,v) = -u^4 + u^2(3v^2+\lambda v+1) + 2\lambda uv(2v+\lambda) + v^2(2v^2+3\lambda v+1), \qquad P_z = 3k_cL_3 + \Psi(m,n).$$

Then $c \mid P_z$ and

$$\Psi(m,n) < P_z < \Psi(n,m) < 4m^2(m+\lambda)^2.$$

If moreover $m \le \frac{3}{2}n$, then $\Psi(m,n) > 0$ and $c \le P_z < 4m^2(m+\lambda)^2$.

Proof. The divisibility comes from the third-order congruence of Lemma 3.3, multiplied by L_3 and reduced modulo c; the bracket from writing P_z as a convex combination of $\Psi(m,n)$ and $\Psi(n,m)$ with weight k_c/H. By Lemma 2.14, $3 \le n < m < l < 2n$; by item 2 of Lemma 3.2, k_c is an integer with $0 < k_c < H$.

We first prove $c \mid P_z$. Write $b = c - 2s + a$ and $t = c - s$, where $s^2 = ac + 1 \equiv 1 \pmod c$ (item 1 of Lemma 2.4), and note that $ck_c = aH + rB_n = a(H - B_n) + (a+r)B_n = aL_3 + sB_n$. Substituting $b \equiv a - 2s$, $t \equiv -s$ and $s^2 \equiv 1 \pmod c$ in A_z, with A_z as in Lemma 3.3, gives

$$A_z \equiv \lambda a^2 L_3(m^2+n^2-1) + 2as\,\Theta - 4(n^3-n)(1+\lambda n) \pmod c,$$
$$\Theta = (m^3-m) + (n^3-n) + 2\lambda n(n^3-n),$$

since $(a-2s)(n^3-n)\big(-2s+\lambda(a-2s)n\big) \equiv (n^3-n)\big(\lambda a^2 n - 2as - 4\lambda asn + 4 + 4\lambda n\big)$. Multiplying by λL_3 and using $aL_3 \equiv -sB_n$ and $s^2 \equiv 1$: $a^2L_3^2(m^2+n^2-1) \equiv B_n^2(m^2+n^2-1)$, $2\lambda asL_3\Theta \equiv -2\lambda B_n\Theta$, and $-4\lambda L_3(n^3-n)(1+\lambda n) = -4L_3\big(\lambda(n^3-n)+n^4-n^2\big)$. Together with $3L_3(k_c-H_2)$ this gives

$$\lambda L_3\big(A_z + 3\lambda(k_c-H_2)\big) \equiv B_n^2(m^2+n^2-1) - 2\lambda B_n\Theta - 4L_3\big(\lambda(n^3-n)+n^4-n^2\big) + 3L_3(k_c-H_2) = P_z \pmod c,$$

the last equality being an identity of polynomials in m, n, k_c for each $\lambda \in \{-1,1\}$. Since $24c \mid A_z + 3\lambda(k_c - H_2)$ by Lemma 3.3, $c \mid P_z$.

We next prove the bracket. Grouping terms by degree and using $\lambda^2 = 1$,

$$\Psi(n,m) - \Psi(m,n) = 3(m^4-n^4) + 3\lambda(m^3+m^2n-mn^2-n^3)$$
$$= 3(m^2-n^2)\big(m^2+n^2+\lambda(m+n)\big) = 3HL_3.$$

Therefore $P_z = \big(1-\frac{k_c}{H}\big)\Psi(m,n) + \frac{k_c}{H}\Psi(n,m)$. Since $0 < k_c < H$ and $L_3 > 0$, $\Psi(m,n) < \Psi(n,m)$ and $\Psi(m,n) < P_z < \Psi(n,m)$. Writing $n = m - e$,

$$\Psi(n,m) = 4m^2(m+\lambda)^2 - e\big(2m(m+\lambda)(m+2\lambda) + (3m^2-\lambda m-1)e - 4me^2 + e^3\big).$$

Because $n < m < 2n$, we have $1 \le e < m/2$, so $4me < 2m^2$ and the bracket exceeds $2m(m-1)(m-2) + (m^2-m-1)e > 0$, as $m \ge 4$. Hence $\Psi(n,m) < 4m^2(m+\lambda)^2$.

We finally treat the case $m \le \frac{3}{2}n$. For real $u \ge n$,

$$\frac{\partial^2\Psi}{\partial u^2}(u,n) = -12u^2 + 2(3n^2+\lambda n+1) \le -6n^2 + 2n + 2 < 0,$$

so $u \mapsto \Psi(u,n)$ is strictly concave on $[n, \frac{3}{2}n]$. At the endpoints $\Psi(n,n) = 4n^2(n+\lambda)^2 > 0$ and $16\,\Psi(\frac{3}{2}n, n) = n^2(59n^2 + 180\lambda n + 100) > 0$, the last because $59n^2 - 180n + 100 > 0$ for $n \geq 3$. Hence $\Psi(m,n) > 0$ for $n < m \leq \frac{3}{2}n$, and then $P_z > \Psi(m,n) > 0$ is a positive multiple of c, so $c \leq P_z < 4m^2(m+\lambda)^2$. For the positivity of $\Psi(m,n)$, the condition $m \leq \frac{3}{2}n$ cannot be replaced by $m < 2n$: $\Psi(50, 26) = -7344$ for $\lambda = 1$ and $\Psi(18, 10) = -432$ for $\lambda = -1$.

□

Lemma 3.5. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$. Then $a + b \leq F_\lambda(m,n)$, where*

$$F_1(m,n) = 4m^2n^2 + m^3 + m^2n - m^2 + mn^2 - 2m + n^3 - n^2,$$
$$F_{-1}(m,n) = 4m^2n^2 - 2m^3 - 2m^2n - 2mn^2 + 2mn + m - 2n^3 + n.$$

Proof. The two *cofactor triples* (Q_a, Q_b, Q_r) and (Q'_a, Q'_b, Q'_r) defined below are cross products of two integer vectors orthogonal to (a, b, r), hence integer multiples of (a, b, r), with positive multipliers g, g'; then $a + b \leq g'a + gb$, and the identity for $g'a + gb$, with $0 < k_c < H$, bounds it by a polynomial of degree 4 in m, n. With the index polynomials and the order-two quotients k_a, k_b, k_c of Convention 3.1, the cofactor triples are given by

$$Q_a = k_b(B_n - 2k_c) + M_2k_c, \qquad Q_b = L_2B_n + M_2H - (2L_2 + M_2)k_c, \qquad Q_r = k_b(k_c - H) + L_2k_c,$$

$$Q'_a = (2L_1 + M_1)k_c - L_1B_n, \qquad Q'_b = M_1(H - k_c) + k_a(2k_c - B_n), \qquad Q'_r = (-k_a)k_c + L_1(H - k_c).$$

By Lemma 2.14, $3 \leq n < m < l < 2n$, so $L_1, L_2, L_3, M_1, M_2, H, B_n$ are positive integers; by item 2 of Lemma 3.2, $k_a, k_b, k_c \in \mathbb{Z}$ with $k_a < 0$, $k_b < 0$, $0 < k_c < H$. In particular $Q_a, Q_b, Q_r, Q'_a, Q'_b, Q'_r$ are integers.

We first prove that the two cofactor triples are positive integer multiples of (a, b, r). By the definitions of k_a, k_b, k_c and $c = a + b + 2r$, the vector (a, b, r) is orthogonal to each of

$$\mathbf{v}_1 = (k_a, -L_1, M_1), \qquad \mathbf{v}_2 = (-L_2, k_b, M_2), \qquad \mathbf{v}_3 = (k_c - H,\ k_c,\ 2k_c - B_n),$$

and $(Q_a, Q_b, Q_r) = -(\mathbf{v}_2 \times \mathbf{v}_3)$, $(Q'_a, Q'_b, Q'_r) = -(\mathbf{v}_1 \times \mathbf{v}_3)$. Direct expansion using $ak_a = bL_1 - rM_1$, $bk_b = aL_2 - rM_2$ and $ck_c = aH + rB_n$ gives

$$bQ_r = rQ_b, \qquad aQ_b = bQ_a, \qquad aQ'_r = rQ'_a, \qquad bQ'_a = aQ'_b.$$

Since $k_a < 0$, $k_b < 0$, $0 < k_c < H$ and $L_1, L_2 > 0$, both summands of $Q_r = (-k_b)(H - k_c) + L_2k_c$ and of $Q'_r = (-k_a)k_c + L_1(H - k_c)$ are positive, so $Q_r, Q'_r > 0$. As $r^2 - ab = 1$, $\gcd(a, r) = \gcd(b, r) = 1$; hence $r \mid Q_r$ (from $bQ_r = rQ_b$) and $r \mid Q'_r$ (from $aQ'_r = rQ'_a$), and with $g = Q_r/r \geq 1$, $g' = Q'_r/r \geq 1$ the four identities give $(Q_a, Q_b, Q_r) = g(a, b, r)$ and $(Q'_a, Q'_b, Q'_r) = g'(a, b, r)$.

We next derive the identity for $g'a + gb$. We have $2L_1 + M_1 = 2l^2 - l + \lambda m$ and $2L_2 + M_2 = 2l^2 - l + \lambda n$, so $(2L_1 + M_1) - (2L_2 + M_2) = \lambda(m - n)$, while $L_2 - L_1 = L_3$. Adding $Q'_a = g'a$ and $Q_b = gb$ cancels l^2 and gives

$$g'a + gb = L_3B_n + M_2H + \lambda(m - n)k_c.$$

We finally prove $a + b \leq F_\lambda(m,n)$. Since $g, g' \geq 1$, $a + b \leq g'a + gb$. Since $l \geq m + 1$, $M_2 \leq 2n^2 + \lambda n - m - 1$; and $1 \leq k_c \leq H - 1$. When $\lambda = 1$, using $(m - n)k_c \leq (m - n)(H - 1)$,

$$g'a + gb \leq L_3B_n + (2n^2 - 1)H - (m - n) = F_1(m,n).$$

When $\lambda = -1$, using $-(m-n)k_c < 0$ and $M_2 \le 2n^2 - n - m - 1$,

$$g'a + gb < L_3 B_n + (2n^2 - n - m - 1)H = F_{-1}(m,n).$$

□

Theorem 3.6. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$. Then*

$$c < 4m^2(m+\lambda)^2 < 8m^4.$$

Proof. The first inequality comes from the quartic bracket of Lemma 3.4 when $m \le \frac{3}{2}n$, and from the quartic bound for $a+b$ of Lemma 3.5 otherwise; the second from $m \ge 4$. By Lemma 2.14, $3 \le n < m < l < 2n$ and $m \ge 4$, so $m \le 2n-2$.

If $m \le \frac{3}{2}n$, then Lemma 3.4 gives $c \le P_z < 4m^2(m+\lambda)^2$.

Suppose now $m > \frac{3}{2}n$, so $n < \frac{2}{3}m$. By item 4 of Lemma 2.4, $c \le 2(a+b)$, and by Lemma 3.5, $a+b \le F_\lambda(m,n)$.

When $\lambda = 1$: $4m^2n^2 < \frac{16}{9}m^4$ and $m^3 + m^2n + mn^2 + n^3 < \big(1 + \frac{2}{3} + \frac{4}{9} + \frac{8}{27}\big)m^3 = \frac{65}{27}m^3$, while the remaining terms of $F_1(m,n)$ are negative, so

$$c \le 2F_1(m,n) < \frac{32}{9}m^4 + \frac{130}{27}m^3 < 4m^4 + 8m^3 < 4m^2(m+1)^2.$$

When $\lambda = -1$: $-2m^2n + 2mn \le 0$, $m - 2mn^2 < 0$ and $n - 2n^3 < 0$, so $F_{-1}(m,n) < 4m^2n^2 - 2m^3 < \frac{16}{9}m^4 - 2m^3$. Moreover $\frac{3}{2}n < m \le 2n-2$ with $n \ge 3$ forces $m \ge 8$: for $n \le 4$ no integer m satisfies $\frac{3}{2}n < m \le 2n-2$, and for $n \ge 5$, $m > \frac{15}{2}$. Hence

$$4m^2(m-1)^2 - c > 4m^2(m-1)^2 - 2\Big(\frac{16}{9}m^4 - 2m^3\Big) = \frac{4}{9}m^2(m^2 - 9m + 9) > 0.$$

Here $m^2 - 9m + 9 = m(m-9) + 9 \ge 1$, as $m \ge 8$. So $c < 4m^2(m+\lambda)^2$ in all cases.

Finally, $m \ge 4$ gives $m^2 - 2m - 1 > 0$, that is $(m+1)^2 < 2m^2$; hence $4m^2(m+\lambda)^2 \le 4m^2(m+1)^2 < 8m^4$. □

The next section does not use it: for close units the gap inequalities take its place.

4 Close Pell units force regularity

This section proves the criterion for close Pell units (Theorem 4.5) and the ratio window that follows from it (Corollary 4.6). Both conditions of the criterion rest on one mechanism, applied to two pairs of units. When b/a is large, β/α is close to 1 and Λ_x is a linear form in $\log(\beta/\alpha)$ and $\log(\alpha^{2(l-m)}D_\lambda)$; when $b-a$ is small compared with $\sqrt{ac}$, γ/β is close to 1 and Λ_z is a linear form in $\log(\gamma/\beta)$ and $\log(\beta^{2(m-n)}E_\lambda)$. The mechanism is proved once, for two abstract numbers (Lemma 4.4), and the criterion checks its conditions in the two cases. All the numbers involved lie in the real biquadratic field $\mathcal{K} = \mathbb{Q}(\sqrt{ab}, \sqrt{ac})$, where we first compute their sizes and heights.

Definition 4.1. For a nonzero algebraic number η of degree $\mathcal{D} = [\mathbb{Q}(\eta) : \mathbb{Q}]$, let $a_\eta \prod_{j=1}^{\mathcal{D}}(X - \eta^{(j)})$, with $a_\eta > 0$, be its primitive irreducible polynomial over $\mathbb{Z}$. Its **absolute logarithmic height** is

$$\mathrm{h}(\eta) = \frac{1}{\mathcal{D}}\Big(\log a_\eta + \sum_{j=1}^{\mathcal{D}} \log\max\big\{1, |\eta^{(j)}|\big\}\Big).$$

Lemma 4.2. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$, with D_λ, E_λ as in Definition 2.16, and put $\mathcal{K} = \mathbb{Q}(\sqrt{ab}, \sqrt{ac})$. Then:*

1. $\frac{1}{2}\log c < \log\alpha < \log c - \log 2$, $\frac{1}{2}\log c + \log 2 < \log\beta < \log c$, *and* $\log\beta - \log\alpha < \log 2 + 4/c$;
2. $\mathcal{K}$ *is a real biquadratic field that contains* $\alpha, \beta, \gamma, D_\lambda, E_\lambda$, *and for* $(e_1, e_2) \in \{-1, 1\}^2$ *it has an embedding with* $\alpha \mapsto \alpha^{e_1}$, $\beta \mapsto \beta^{e_2}$, $\gamma \mapsto \gamma^{e_1 e_2}$;
3. *for integers* i, j, $\mathrm{h}(\beta^i\alpha^j) = \frac{1}{2}\max(|i|\log\beta, |j|\log\alpha)$, *in particular* $\mathrm{h}(\alpha) = \frac{1}{2}\log\alpha$ *and* $\mathrm{h}(\beta/\alpha) = \frac{1}{2}\log\beta$; *and* $\mathrm{h}(\gamma/\beta) = \frac{1}{2}\log\gamma$; *moreover* β/α *and* γ/β *have degree* 4 *over* $\mathbb{Q}$;
4. $0 < \log D_\lambda < \min\{\log 4,\ 2\sqrt{a/b}\}$, $N_{\mathcal{K}/\mathbb{Q}}(D_\lambda) = \left(\frac{c(b-a)}{b(c-a)}\right)^2 \in (0, 1)$, *and* $\mathrm{h}(D_\lambda) < \log c$;
5. $0 < \log E_\lambda < 2(b-a)/\sqrt{ac}$, $N_{\mathcal{K}/\mathbb{Q}}(E_\lambda) = \left(\frac{b(c-a)}{a(c-b)}\right)^2 > 1$, *and* $\mathrm{h}(E_\lambda) < \log\beta$ *if* $b \le \frac{3}{2}a$;
6. *The numbers* α, β/α *and* D_λ *exceed* 1 *and are multiplicatively independent, and so do* γ/β *and* $\beta^{2(m-n)}E_\lambda$.

Proof. The size estimates in items 1, 4 and 5 are elementary consequences of the identities of an Euler triple; the norms, heights, degrees and independence statements come from the four embeddings of $\mathcal{K}$ of item 2, which invert α and β independently. We use the identities of Lemma 2.4 throughout: $s = a + r$, $t = b + r$, $s^2 = ac + 1$, $t^2 = bc + 1$, $a < r < b$ and $4a < c \le 2(a + b)$; as $c = a + b + 2r$, these give $2r \le a + b$, $c \ge 4r$ and $c < 4b$, and $c > 4a$ gives $\sqrt{a} < \frac{1}{2}\sqrt{c}$. By Lemma 2.14, $n < m$.

We first prove item 1. Since $c \ge 4r$, $\alpha < 2r \le c/2$, so $\log\alpha < \log c - \log 2$. Next $\alpha^2 = 2ab + 1 + 2r\sqrt{ab}$, so $\alpha^2 - c = (2ab - a - b) + 1 + 2r(\sqrt{ab} - 1) > 0$ and $\log\alpha > \frac{1}{2}\log c$. Since $s^2 = ac + 1$,

$$2\sqrt{c} \le 2\sqrt{ac} < \beta < 2s = 2a + 2r = c - (b - a) < c,$$

so $\frac{1}{2}\log c + \log 2 < \log\beta < \log c$. Finally $\alpha = 2r - \alpha^{-1} > 2r - r^{-1}$ and $s/r = 1 + a/r < 2$, so, as $4r^2 = 4ab + 4 > 2(a + b) \ge c$,

$$\log\beta - \log\alpha < \log\frac{2s}{2r - r^{-1}} = \log\frac{s}{r} - \log\Big(1 - \frac{1}{2r^2}\Big) < \log 2 + \frac{1}{r^2} < \log 2 + \frac{4}{c},$$

using $-\log(1 - x) \le x/(1 - x) \le 2x$ for $0 < x \le \frac{1}{2}$.

We next prove item 2. The integers ab, ac, bc are not squares (Lemma 2.4, item 5), and $ab \cdot ac = a^2 \cdot bc$; hence $\mathcal{K}$ is a real biquadratic field with the four embeddings $\sigma_{e_1,e_2}\colon \sqrt{ab} \mapsto e_1\sqrt{ab}$, $\sqrt{ac} \mapsto e_2\sqrt{ac}$, and $\sqrt{bc} = \sqrt{ab}\sqrt{ac}/a$ lies in $\mathcal{K}$ and is sent to $e_1e_2\sqrt{bc}$. The units $\alpha = r + \sqrt{ab}$, $\beta = s + \sqrt{ac}$ and $\gamma = t + \sqrt{bc}$ lie in $\mathcal{K}$, and $\alpha^{-1} = r - \sqrt{ab}$, $\beta^{-1} = s - \sqrt{ac}$, $\gamma^{-1} = t - \sqrt{bc}$ (Lemma 2.4, item 5); so σ_{e_1,e_2} sends $\alpha \mapsto \alpha^{e_1}$, $\beta \mapsto \beta^{e_2}$ and $\gamma \mapsto \gamma^{e_1e_2}$. The numbers D_λ and E_λ are quotients of sums of $\pm\sqrt{ab}, \pm\sqrt{ac}, \sqrt{bc}$, so they lie in $\mathcal{K}$ as well.

We next prove item 3. By item 2, the conjugates of the unit $\beta^i\alpha^j$ are $\exp(\pm i\log\beta \pm j\log\alpha)$ with independent signs, so

$$4\,\mathrm{h}(\beta^i\alpha^j) = |i\log\beta + j\log\alpha| + |i\log\beta - j\log\alpha| = 2\max(|i|\log\beta, |j|\log\alpha).$$

With $\beta > \alpha > 1$ (as $s > r$ and $\sqrt{ac} > \sqrt{ab}$) this gives $\mathrm{h}(\alpha) = \frac{1}{2}\log\alpha$ and $\mathrm{h}(\beta/\alpha) = \frac{1}{2}\log\beta$. Likewise, by item 2 the four conjugates of the unit γ/β are $(\gamma/\beta)^{\pm 1}$ and $(\beta\gamma)^{\pm 1}$; as $\gamma > \beta > 1$ (because $t > s$ and $\sqrt{bc} > \sqrt{ac}$), $\mathrm{h}(\gamma/\beta) = \frac{1}{4}\big(\log(\gamma/\beta) + \log(\beta\gamma)\big) = \frac{1}{2}\log\gamma$. For the degrees, the images $\beta^{e_2}\alpha^{-e_1}$ of β/α under the four embeddings of item 2 are β/α, $\alpha\beta$, $(\alpha\beta)^{-1}$, α/β, which

are distinct because $\beta > \alpha > 1$; and the images $\gamma^{e_1e_2}\beta^{-e_2}$ of γ/β are γ/β, β/γ, $(\beta\gamma)^{-1}$, $\beta\gamma$ (for $(e_1,e_2) = (1,1),(1,-1),(-1,1),(-1,-1)$), which are distinct because $\gamma > \beta > 1$. So β/α and γ/β have degree 4.

We next prove item 4. Dividing numerator and denominator in Definition 2.16 by $\sqrt{bc}$ gives $D_\lambda = (1+\sqrt{a/b})/(1+\lambda\sqrt{a/c})$. Since $c - (\sqrt{a}+\sqrt{b})^2 = 2(r-\sqrt{ab}) > 0$, one has $\sqrt{a/c} < \sqrt{a}/(\sqrt{a}+\sqrt{b})$, i.e. $1-\sqrt{a/c} > (1+\sqrt{a/b})^{-1}$. Hence $1 < D_\lambda \le D_{-1} < (1+\sqrt{a/b})^2$, where $D_\lambda > 1$ because $\sqrt{a/b} > \sqrt{a/c}$. So $0 < \log D_\lambda < 2\log(1+\sqrt{a/b})$, which is less than $2\sqrt{a/b}$ and than $\log 4$. The numerator $N_x = \sqrt{bc}+\sqrt{ac}$ and the denominator $M_x = \sqrt{bc}+\lambda\sqrt{ab}$ of D_λ are algebraic integers, and by item 2

$$\sigma_{e_1,e_2}N_x = e_2(e_1\sqrt{bc}+\sqrt{ac}), \quad |\sigma_{e_1,e_2}N_x| = \sqrt{bc}+e_1\sqrt{ac},$$
$$\sigma_{e_1,e_2}M_x = e_1(e_2\sqrt{bc}+\lambda\sqrt{ab}), \quad |\sigma_{e_1,e_2}M_x| = \sqrt{bc}+\lambda e_2\sqrt{ab}.$$

The inner factors $e_1\sqrt{bc}+\sqrt{ac}$ and $e_2\sqrt{bc}+\lambda\sqrt{ab}$ have signs e_1 and e_2, so $\sigma_{e_1,e_2}N_x$ and $\sigma_{e_1,e_2}M_x$ both have sign e_1e_2. Hence every conjugate of D_λ is positive, $N_{\mathcal{K}/\mathbb{Q}}(N_x) = (bc-ac)^2$ and $N_{\mathcal{K}/\mathbb{Q}}(M_x) = (bc-ab)^2$, which gives the norm; it lies in $(0,1)$ because $b(c-a)-c(b-a) = a(c-b) > 0$. Since $ac > ab$, the four values of $\max(|\sigma_{e_1,e_2}N_x|, |\sigma_{e_1,e_2}M_x|)$ are $\sqrt{bc}+\sqrt{ac}$ (for $e_1 = 1$, twice), $\sqrt{bc}+\sqrt{ab}$ and $\sqrt{bc}-\sqrt{ab}$ (for $e_1 = -1$). By the product formula, $4\,\mathrm{h}(N_x/M_x)$ is the sum of $\log\max(\|N_x\|, \|M_x\|)$ over the normalized absolute values $\|\cdot\|$ of $\mathcal{K}$; the finite places contribute at most 0 because N_x, M_x are algebraic integers, and the four real places give

$$4\,\mathrm{h}(D_\lambda) \le 2\log(\sqrt{bc}+\sqrt{ac}) + \log(bc-ab) = \log\big(c(\sqrt{a}+\sqrt{b})^2\big) + \log\big(b(c-a)\big) < 4\log c,$$

using $(\sqrt{a}+\sqrt{b})^2 < c$ and $b(c-a) < c^2$.

We next prove item 5. Since $\sqrt{bc} > \sqrt{ac} > \sqrt{ab}$, $E_\lambda - 1 = (\sqrt{bc}-\sqrt{ac})/(\sqrt{ac}+\lambda\sqrt{ab}) > 0$. Put $u = \sqrt{a}$, $v = \sqrt{b}$ and $w = \sqrt{c}$, so that $u < v$ and $u+v < w < 2v$ (as $(\sqrt{a}+\sqrt{b})^2 < c < 4b$), and $E_\lambda = \frac{v(w+\lambda u)}{u(w+\lambda v)}$. For $\lambda = 1$, $E_1 < v/u$, so $\log E_1 < \frac{v-u}{u} \le \frac{2(v^2-u^2)}{uw}$, the last step because $w < 2v < 2(u+v)$. For $\lambda = -1$, using $\log(1+\rho) < \rho$ for $\rho > 0$,

$$\log E_{-1} = \log\frac{v}{u} + \log\Big(1+\frac{v-u}{w-v}\Big) < (v-u)\Big(\frac{1}{u}+\frac{1}{w-v}\Big) \le \frac{2(v^2-u^2)}{uw},$$

where the last inequality is equivalent to $w^2-(u+3v)w+2v(u+v) \le 0$, that is, to $(w-u-v)(w-2v) \le 0$. Since $v^2-u^2 = b-a$ and $uw = \sqrt{ac}$, in both cases $0 < \log E_\lambda < 2(b-a)/\sqrt{ac}$.

The numerator $N_z = \sqrt{bc}+\lambda\sqrt{ab}$ and the denominator $M_z = \sqrt{ac}+\lambda\sqrt{ab}$ of E_λ are algebraic integers, and by item 2 $|\sigma_{e_1,e_2}N_z| = \sqrt{bc}+\lambda e_2\sqrt{ab}$ and $|\sigma_{e_1,e_2}M_z| = \sqrt{ac}+\lambda e_1e_2\sqrt{ab}$, both positive. Hence $N_{\mathcal{K}/\mathbb{Q}}(N_z) = (bc-ab)^2 = b^2(c-a)^2$ and $N_{\mathcal{K}/\mathbb{Q}}(M_z) = (ac-ab)^2 = a^2(c-b)^2$; since $b(c-a)-a(c-b) = c(b-a) > 0$, the norm of E_λ exceeds 1. For $e_1 = 1$ the larger of $|\sigma_{e_1,e_2}N_z|$ and $|\sigma_{e_1,e_2}M_z|$ is $|\sigma_{e_1,e_2}N_z|$, and the product of its two values ($e_2 = \pm 1$) is $bc-ab = b(c-a)$; for $e_1 = -1$ both are at most $\sqrt{bc}+\sqrt{ab} = \sqrt{b}(\sqrt{c}+\sqrt{a})$. By the product formula, the finite places contributing at most 0,

$$4\,\mathrm{h}(E_\lambda) \le \log\big(b(c-a)\big) + \log\big(b(\sqrt{c}+\sqrt{a})^2\big).$$

When $b \le \frac{3}{2}a$, one has $b(c-a) < bc \le \frac{3}{2}ac$ and, as $(\sqrt{c}+\sqrt{a})^2 < \frac{9}{4}c$, $b(\sqrt{c}+\sqrt{a})^2 < \frac{9}{4}bc \le \frac{27}{8}ac$; so $4\,\mathrm{h}(E_\lambda) < \log\big(\frac{81}{16}(ac)^2\big) < \log\beta^4$, because $\beta = s+\sqrt{ac} > 2\sqrt{ac}$. Hence $\mathrm{h}(E_\lambda) < \log\beta$.

We finally prove item 6. Here $\alpha > 1$, $\beta/\alpha > 1$ (as $s > r$ and $\sqrt{ac} > \sqrt{ab}$) and $D_\lambda > 1$ (item 4). If $\alpha^i(\beta/\alpha)^j D_\lambda^k = 1$ with integers i,j,k, taking norms gives $N_{\mathcal{K}/\mathbb{Q}}(D_\lambda)^k = 1$, as the units α, β have norm 1 by item 2; so $k = 0$ by item 4. Then $\beta^j\alpha^{i-j} = 1$, and the embedding $\sigma_{1,-1}$ gives

$\beta^{-j}\alpha^{i-j}=1$, whence $\beta^{2j}=1$, $j=0$ and $i=0$. Next $\gamma/\beta>1$ because $t>s$ and $\sqrt{bc}>\sqrt{ac}$, and $\beta^{2(m-n)}E_\lambda>1$ because $m>n$ and $E_\lambda>1$ (item 5). If $(\gamma/\beta)^i\big(\beta^{2(m-n)}E_\lambda\big)^j=1$ with integers i,j, taking norms gives $N_{\mathcal{K}/\mathbb{Q}}(E_\lambda)^j=1$, as the units β,γ have norm 1 by item 2; so $j=0$ by item 5, and then $i=0$ because $\gamma/\beta>1$. □

The bound $\mathrm{h}(D_\lambda)<\log c$ of item 4 is essentially sharp: for the Euler triples $\{3,5,16\}$ and $\{1,120,143\}$ an exact computation gives $\mathrm{h}(D_\lambda)\approx 0.875\log c$ and $\mathrm{h}(D_\lambda)\approx 0.991\log c$, for both values of λ. It enters the criterion through the height of $\alpha^{2(l-m)}D_\lambda$ in the case of large b/a. The lower bound that we play against the smallness of the forms is Laurent's theorem on linear forms in two logarithms [22], quoted in the form we use.

Theorem 4.3. *Let $\eta_1,\eta_2>1$ be real algebraic numbers that are multiplicatively independent, put $\mathcal{D}=[\mathbb{Q}(\eta_1,\eta_2):\mathbb{Q}]$, let b_1,b_2 be positive integers, and*

$$\Lambda_L=b_2\log\eta_2-b_1\log\eta_1.$$

Let $\rho>1$ and $\frac13\le\mu\le1$ be real, and put $\sigma_L=\frac{1+2\mu-\mu^2}{2}$ and $\lambda_L=\sigma_L\log\rho$. With the height h *of Definition 4.1, let A_1,A_2 be real numbers with*

$$A_i\ge\max\big\{1,\ (\rho-1)\log\eta_i+2\mathcal{D}\,\mathrm{h}(\eta_i)\big\}\quad(i=1,2),\qquad A_1A_2\ge\lambda_L^2,$$

and let h_L be a real number with

$$h_L\ge\max\Big\{\mathcal{D}\Big(\log\Big(\frac{b_1}{A_2}+\frac{b_2}{A_1}\Big)+\log\lambda_L+1.75\Big)+0.06,\ \lambda_L,\ \frac{\mathcal{D}\log2}{2}\Big\}.$$

Put

$$\mathcal{H}=\frac{h_L}{\lambda_L}+\frac{1}{\sigma_L},\qquad \omega_L=2\Big(1+\sqrt{1+\frac{1}{4\mathcal{H}^2}}\Big),\qquad \theta_L=\sqrt{1+\frac{1}{4\mathcal{H}^2}}+\frac{1}{2\mathcal{H}},$$

$$\mathcal{C}=\frac{\mu}{\lambda_L^3\sigma_L}\Big(\frac{\omega_L}{6}+\frac12\sqrt{\frac{\omega_L^2}{9}+\frac{8\lambda_L\omega_L^{5/4}\theta_L^{1/4}}{3\sqrt{A_1A_2}\sqrt{\mathcal{H}}}+\frac43\Big(\frac{1}{A_1}+\frac{1}{A_2}\Big)\frac{\lambda_L\omega_L}{\mathcal{H}}}\Big)^2,\qquad \mathcal{C}'=\sqrt{\frac{\mathcal{C}\sigma_L\omega_L\theta_L}{\lambda_L^3\mu}}.$$

Then

$$\log|\Lambda_L|\ge-\mathcal{C}\,(h_L+\log\rho)^2A_1A_2-\sqrt{\omega_L\theta_L}\,(h_L+\log\rho)-\log\big(\mathcal{C}'(h_L+\log\rho)^2A_1A_2\big).$$

Proof. This is [22, Theorem 2, p. 327], in the case of two real numbers greater than 1 with their real logarithms; there $\mathcal{D}=[\mathbb{Q}(\eta_1,\eta_2):\mathbb{Q}]/[\mathbb{R}(\eta_1,\eta_2):\mathbb{R}]$, which is the degree in this case, and $\lambda_L/\sigma_L=\log\rho$. □

The next lemma is the crux of the section. It concerns two numbers η_1,η_2, the first close to 1 and the second of height linear in an integer g, and it excludes a very small form $\log\eta_2-2k\log\eta_1$ when $k>gT\xi$; its two sets of constants serve the two cases of the criterion.

Lemma 4.4. *Let $\eta_1,\eta_2>1$ be real algebraic numbers that are multiplicatively independent, with $[\mathbb{Q}(\eta_1,\eta_2):\mathbb{Q}]=4$, and let*

$$(T,\xi_0,h_0,C)=(3355,\ \log6710,\ 2,\ 4.01)\qquad\text{or}\qquad(T,\xi_0,h_0,C)=(3075,\ \log12300,\ 1,\ 2).$$

There do not exist a real number $\xi>\xi_0$ and integers $g,k\ge1$ such that

$$\log\eta_1<\frac{1}{T},\qquad \mathrm{h}(\eta_1)<\frac12\Big(\xi+\frac1T\Big),\qquad \log\eta_2<2g\xi+\frac{2}{T},\qquad \mathrm{h}(\eta_2)<(g+h_0)\xi,\qquad k>gT\xi,$$

and

$$0 < \log\eta_2 - 2k\log\eta_1 < C\,e^{-4k\xi}.$$

Proof. We play the upper bound $Ce^{-4k\xi}$ of the last condition against Laurent's lower bound (Theorem 4.3). The first four conditions allow Laurent's parameters A_1 and A_2 of order ξ and $g\xi$, so that the lower bound is roughly exponential in $g\xi^2$ times the square of $\log(k/(g\xi))$, while the upper bound is exponential in $k\xi$; and the condition $k > gT\xi$ makes $k/(g\xi)$ too large for both bounds to hold.

Suppose that $\xi > \xi_0$ and $g, k \geq 1$ satisfy all the displayed conditions, and put $\Lambda_L = \log\eta_2 - 2k\log\eta_1$. We derive a contradiction from Theorem 4.3, applied with $b_1 = 2k$, $b_2 = 1$, $\mathcal{D} = [\mathbb{Q}(\eta_1,\eta_2):\mathbb{Q}] = 4$, $\rho = 37$ and $\mu = \frac{63}{100}$, so that $\sigma_L = \frac{1+2\mu-\mu^2}{2} = 0.93155$ and $\lambda_L = \sigma_L \log 37 = 3.36375\ldots$.

We first fix the parameters A_1, A_2, h_L and check the hypotheses of Theorem 4.3. Put $(\chi_1,\chi_2) = (4.0014,\, 16.0025)$ in the first case and $(\chi_1,\chi_2) = (4.0015,\, 8.0025)$ in the second, and

$$A_1 = \chi_1\xi, \qquad A_2 = (80g+\chi_2)\xi.$$

Laurent's condition with $\rho = 37$, $\mathcal{D} = 4$ reads $A_i \geq 36\log\eta_i + 8\,\mathrm{h}(\eta_i)$, with the height h of Definition 4.1; and since $\xi > \xi_0$, the first four conditions give

$$36\log\eta_1 + 8\,\mathrm{h}(\eta_1) < 4\xi + \frac{40}{T} < \Big(4 + \frac{40}{T\xi_0}\Big)\xi < A_1,$$

$$36\log\eta_2 + 8\,\mathrm{h}(\eta_2) < (80g+8h_0)\xi + \frac{72}{T} < \Big(80g + 8h_0 + \frac{72}{T\xi_0}\Big)\xi < A_2,$$

and $A_1, A_2 > 1$, $A_1A_2 > 320\,\xi_0^2 > \lambda_L^2$. Put $\delta_0 = 1/(\chi_1\xi_0)$, $\ell_* = \log\lambda_L + 1.75 + \frac14(0.06 + \log 37) = 3.88078\ldots$, and

$$Y = \frac{2k}{(80g+\chi_2)\xi}, \qquad \ell_Y = \log(Y+\delta_0) + \ell_*,$$
$$h_L = 4\ell_Y - \log 37 = 4\big(\log(Y+\delta_0) + \log\lambda_L + 1.75\big) + 0.06.$$

Since $b_1/A_2 + b_2/A_1 = Y + 1/(\chi_1\xi) < Y + \delta_0$, the number h_L satisfies the first lower bound required of it in Theorem 4.3. Next, the condition $k > gT\xi$, which enters only here, and $80g + \chi_2 \leq (80+\chi_2)g$ give

$$Y > Y_0 := \frac{2T}{80+\chi_2},$$
$$\text{that is} \quad Y_0 = \frac{6710}{96.0025} = 69.89401\ldots \quad \text{or} \quad Y_0 = \frac{6150}{88.0025} = 69.88437\ldots,$$

so $\ell_Y > \ell_{Y_0} > 8.12$ and $h_L > 28$, which exceeds λ_L and $\frac{\mathcal{D}\log 2}{2} = 2\log 2$. As $\lambda_L/\sigma_L = \log 37$, the quantity $\mathcal{H}$ of Theorem 4.3 is $\mathcal{H} = (h_L + \log 37)/\lambda_L = 4\ell_Y/\lambda_L$, and since $\Lambda_L > 0$ the theorem gives

$$\log\Lambda_L \geq -16\,\mathcal{C}\,\ell_Y^2 A_1A_2 - 4\sqrt{\omega_L\theta_L}\,\ell_Y - \log\big(16\,\mathcal{C}'\ell_Y^2 A_1A_2\big). \tag{1}$$

We next replace the auxiliary functions of (1) by constants. The functions ω_L and θ_L of Theorem 4.3 decrease as $\mathcal{H}$ increases, so $\mathcal{C}$ decreases as $\mathcal{H}$, A_1 or A_2 increases, and so does $\mathcal{C}'$. We have $\mathcal{H} \geq \mathcal{H}_0 := 4\ell_{Y_0}/\lambda_L$, $A_1 \geq A_{1,0} := \chi_1\xi_0$ and $A_2 \geq A_{2,0} := (80+\chi_2)\xi_0$. Let $\omega_{L,0}, \theta_{L,0}, \mathcal{C}_0, \mathcal{C}_0'$ denote the values of $\omega_L, \theta_L, \mathcal{C}, \mathcal{C}'$ at $(\mathcal{H}_0, A_{1,0}, A_{2,0})$; then $\omega_L\theta_L \leq \omega_{L,0}\theta_{L,0}$, $\mathcal{C} \leq \mathcal{C}_0$ and $\mathcal{C}' \leq \mathcal{C}_0'$.

We now turn (1) and the upper bound for Λ_L into an inequality $Y < \Theta(Y)$. By hypothesis $\log \Lambda_L < \log C - 4k\xi$. Combining this with (1) and the three bounds just obtained, and dividing by $2A_2\xi = 2\Xi$ with $\Xi = (80g + \chi_2)\xi^2$, we get, since $4k\xi/(2\Xi) = Y$ and $A_1A_2/(2A_2\xi) = \chi_1/2$,

$$Y < 8\chi_1\mathcal{C}_0\,\ell_Y^2 + \frac{2\sqrt{\omega_{L,0}\theta_{L,0}}\,\ell_Y}{\Xi} + \frac{\log\bigl(16\,\mathcal{C}_0'\ell_Y^2\chi_1\Xi\bigr) + \log C}{2\Xi}.$$

Put $\Xi_0 = (80 + \chi_2)\xi_0^2$, so that $\Xi \geq \Xi_0$. The function $u \mapsto \log(Qu)/u$ decreases for $Qu \geq e$, and $Q = 16\,\mathcal{C}_0'\ell_Y^2\chi_1$ satisfies $Q\Xi_0 > 2 \cdot 10^6$; moreover $\log C > 0$. Hence each of the last two terms is largest at $\Xi = \Xi_0$, and

$$Y < \Theta(Y) := \psi_2\ell_Y^2 + \psi_1\ell_Y + \psi_0 \log \ell_Y + \psi_*,$$

$$\psi_2 = 8\chi_1\mathcal{C}_0, \qquad \psi_1 = \frac{2\sqrt{\omega_{L,0}\theta_{L,0}}}{\Xi_0}, \qquad \psi_0 = \frac{1}{\Xi_0}, \qquad \psi_* = \frac{\log\bigl(16\,C\,\mathcal{C}_0'A_{1,0}A_{2,0}\bigr)}{2\Xi_0},$$

where $\ell_Y = \log(Y + \delta_0) + \ell_*$ is now read as a function of the real variable $Y \geq Y_0$.

We next show that $\Theta(Y)/Y$ is strictly decreasing for $Y \geq Y_0$. The coefficients ψ_2, ψ_1, ψ_0 are positive, and $\psi_* > 0$ by the evaluation below. Since $d\ell_Y/dY = 1/(Y + \delta_0) < 1/Y$ and $\ell_Y \geq \ell_{Y_0} > 2$,

$$Y\Theta'(Y) < 2\psi_2\ell_Y + \psi_1 + \frac{\psi_0}{\ell_Y} \leq \psi_2\ell_Y^2 + \psi_1\ell_Y + \psi_0 \log \ell_Y < \Theta(Y),$$

because $2\ell_Y \leq \ell_Y^2$, $1 \leq \ell_Y$ and $1/\ell_Y < \log \ell_Y$ for $\ell_Y \geq 2$. Hence $\frac{d}{dY}\bigl(\Theta(Y)/Y\bigr) = \bigl(Y\Theta'(Y) - \Theta(Y)\bigr)/Y^2 < 0$.

Finally we evaluate at Y_0. All constants above are explicit, and their values were computed in interval arithmetic with 256-bit endpoints, every comparison below holding for the full intervals. In the first case $\mathcal{H}_0 = 9.66560\ldots$, $\omega_{L,0} = 4.00267\ldots$, $\theta_{L,0} = 1.05306\ldots$, $\mathcal{C}_0 = 0.0329567\ldots$, $\mathcal{C}_0' = 0.0734636\ldots$, $\psi_2 = 1.054986\ldots$, $\psi_1 = 5.5089\ldots \cdot 10^{-4}$, $\psi_0 = 1.3416\ldots \cdot 10^{-4}$, $\psi_* = 7.9515\ldots \cdot 10^{-4}$, and

$$\Theta(Y_0) = 69.70554\ldots < 69.89401\ldots = Y_0.$$

In the second case $\mathcal{H}_0 = 9.66541\ldots$, $\omega_{L,0} = 4.00267\ldots$, $\theta_{L,0} = 1.05306\ldots$, $\mathcal{C}_0 = 0.0329086\ldots$, $\mathcal{C}_0' = 0.0734100\ldots$, $\psi_2 = 1.053472\ldots$, $\psi_1 = 5.2611\ldots \cdot 10^{-4}$, $\psi_0 = 1.2812\ldots \cdot 10^{-4}$, $\psi_* = 7.1772\ldots \cdot 10^{-4}$, and

$$\Theta(Y_0) = 69.60241\ldots < 69.88437\ldots = Y_0.$$

In both cases $Q\Xi_0 > 2 \cdot 10^6$ at $\ell_Y = \ell_{Y_0}$, which gives it for every larger ℓ_Y. Since $\Theta(Y)/Y$ decreases, $\Theta(Y) < Y$ for every $Y \geq Y_0$, which contradicts $Y < \Theta(Y)$ at our $Y > Y_0$.

□

Theorem 4.5. *Let $\{a, b, c\}$ be an Euler triple with*

$$b \geq 3355^2 a \qquad \text{or} \qquad \sqrt{ac} \geq 3075\,(b - a).$$

Then $\{a, b, c\}$ has no irregular extension.

Proof. Suppose that d is an irregular extension of $\{a, b, c\}$, and let (λ, l, m, n) be its index system (Proposition 2.11), with the linear forms Λ_x, Λ_z, the numbers D_λ, E_λ and the gap ratios R_x, R_z of Definition 2.16. By Lemma 2.14, $n < m < l$. In each of the two cases we exhibit numbers $\eta_1, \eta_2, \xi, g, k$ that satisfy all the conditions which Lemma 4.4 excludes; the first case uses the

linear form Λ_x, the second the linear form Λ_z. Throughout, h is the height of Definition 4.1, and we use $\mathrm{h}(uv) \le \mathrm{h}(u) + \mathrm{h}(v)$.

By item 2 of Lemma 4.2, the numbers $\alpha, \beta, \gamma, D_\lambda, E_\lambda$ lie in the real biquadratic field $\mathcal{K} = \mathbb{Q}(\sqrt{ab}, \sqrt{ac})$.

The case $b \ge 3355^2 a$. Put

$$\eta_1 = \frac{\beta}{\alpha}, \qquad \eta_2 = \alpha^{2(l-m)} D_\lambda, \qquad \xi = \log \alpha, \qquad g = l - m \ge 1, \qquad k = m,$$

and $(T, \xi_0, h_0, C) = (3355, \log 6710, 2, 4.01)$. We check the conditions of Lemma 4.4.

- Since $\sqrt{ab} \ge 3355a \ge 3355$ and $r > \sqrt{ab}$, we have $\alpha > 2\sqrt{ab} \ge 6710$, so $\xi > \xi_0$.
- By Lemma 4.2 (item 6), α, β/α and D_λ exceed 1 and are multiplicatively independent; hence $\eta_1, \eta_2 > 1$, and $\eta_1^i \eta_2^j = 1$ with integers i, j forces $i = 2gj = j = 0$, so η_1, η_2 are multiplicatively independent. By Lemma 4.2 (item 3), η_1 has degree 4, so $[\mathbb{Q}(\eta_1, \eta_2) : \mathbb{Q}] = 4$ as $\mathbb{Q}(\eta_1, \eta_2) \subseteq \mathcal{K}$.
- By Lemma 2.18 (item 2), $\log \eta_1 < \sqrt{a/b} \le 1/T$; by Lemma 4.2 (item 3), $\mathrm{h}(\eta_1) = \frac{1}{2} \log \beta = \frac{1}{2}(\xi + \log \eta_1) < \frac{1}{2}(\xi + 1/T)$.
- By Lemma 4.2 (item 4), $\log \eta_2 = 2g\xi + \log D_\lambda < 2g\xi + 2\sqrt{a/b} \le 2g\xi + 2/T$. By items 3, 4 and 1 of Lemma 4.2, $\mathrm{h}(\eta_2) \le \mathrm{h}(\alpha^{2g}) + \mathrm{h}(D_\lambda) < g\xi + \log c < (g+2)\xi$, since $\log c < 2 \log \alpha$.
- By Lemma 2.18 (item 3), $k = m > (l-m) R_x = g\sqrt{b/a}\, \xi \ge gT\xi$.
- $\log \eta_2 - 2k \log \eta_1 = 2l \log \alpha - 2m \log \beta + \log D_\lambda = \Lambda_x$, and by Lemma 2.18 (item 4) $0 < \Lambda_x < 4.01\, \beta^{-4m} < 4.01\, e^{-4k\xi}$, as $\beta > \alpha$.

This contradicts Lemma 4.4.

The case $\sqrt{ac} \ge 3075(b-a)$. Put

$$\eta_1 = \frac{\gamma}{\beta}, \qquad \eta_2 = \beta^{2(m-n)} E_\lambda, \qquad \xi = \log \beta, \qquad g = m - n \ge 1, \qquad k = n,$$

and $(T, \xi_0, h_0, C) = (3075, \log 12300, 1, 2)$. We first note that $b < \frac{3}{2}a$: by Lemma 2.4 (item 4), $c \le 2(a+b) < 4b$, so $\sqrt{ac} < 2b$ and $b - a \le \sqrt{ac}/3075 < 2b/3075$, whence $a > \frac{3073}{3075} b > \frac{2}{3} b$. We check the conditions of Lemma 4.4.

- Since $b - a \ge 2$ (Lemma 2.4, item 4) and $s > \sqrt{ac}$, we have $\beta > 2\sqrt{ac} \ge 6150(b-a) \ge 12300$, so $\xi > \xi_0$.
- By Lemma 4.2 (item 6), $\eta_1, \eta_2 > 1$ and they are multiplicatively independent. By Lemma 4.2 (item 3), η_1 has degree 4, so $[\mathbb{Q}(\eta_1, \eta_2) : \mathbb{Q}] = 4$ as $\mathbb{Q}(\eta_1, \eta_2) \subseteq \mathcal{K}$.
- By Lemma 2.18 (item 2), $\log \eta_1 < (b-a)/\sqrt{ac} \le 1/T$; by Lemma 4.2 (item 3), $\mathrm{h}(\eta_1) = \frac{1}{2} \log \gamma = \frac{1}{2}(\xi + \log \eta_1) < \frac{1}{2}(\xi + 1/T)$.
- By Lemma 4.2 (item 5), $\log \eta_2 = 2g\xi + \log E_\lambda < 2g\xi + 2(b-a)/\sqrt{ac} \le 2g\xi + 2/T$. By items 3 and 5 of Lemma 4.2, the latter applicable as $b \le \frac{3}{2}a$, $\mathrm{h}(\eta_2) \le \mathrm{h}(\beta^{2g}) + \mathrm{h}(E_\lambda) < g\xi + \xi$.
- By Lemma 2.18 (item 3), $k = n > (m-n) R_z = g \frac{\sqrt{ac}}{b-a}\, \xi \ge gT\xi$.
- $\log \eta_2 - 2k \log \eta_1 = 2m \log \beta - 2n \log \gamma + \log E_\lambda = \Lambda_z$, and by Lemma 2.18 (item 5) $0 < \Lambda_z < 2\beta^{-4n} = 2e^{-4k\xi}$.

This contradicts Lemma 4.4. Hence $\{a, b, c\}$ has no irregular extension. □

Corollary 4.6. *If an Euler triple $\{a, b, c\}$ has an irregular extension, then $1+\frac{1}{1538} < \frac{b}{a} < 3355^2$.*

Proof. By Theorem 4.5, $b < 3355^2 a$ and $\sqrt{ac} < 3075(b-a)$. By Lemma 2.4 (item 4), $c > 4a$, so $\sqrt{ac} > 2a$. Hence $2a < 3075(b-a)$, that is $b/a > 1 + \frac{2}{3075} > 1 + \frac{1}{1538}$. □

The heights of Lemma 4.2 and Laurent's theorem are used again in Section 7.

5 Regularity from pair coordinates

This section proves the pair-coordinate criterion (Theorem 5.19). The key idea is that an Euler triple, written in pair coordinates, falls into the setting of Rickert's simultaneous approximations to square roots [26]. In a pair representation $a = p_1 q_1$, $b = p_2 q_2$ with $p_1 q_2 - p_2 q_1 = \pm 2$, the numbers $\sqrt{a/c}$ and $\sqrt{b/c}$, after rescaling, become square roots $\sqrt{1 + a_j/N}$ with integer shifts a_j and an integer N. The hypergeometric method then gives them an effective simultaneous approximation measure (Theorem 5.14), with an exponent below 2 exactly when $40p_3^2 < \omega p_1 q_3$, while the common term z of an irregular extension approximates them with exponent 2. Comparing the two exponents caps the index m (Lemma 5.18); under the hypotheses of the criterion the cap is a multiple of $\log c$, against the floors for m given by the quartic index floor (Theorem 3.6) and, in the first case, by Lemma 5.17.

The section has three parts: Subsection 5.1 states the method for arbitrary integer shifts, Subsection 5.2 applies it to a pair representation, and Subsection 5.3 bounds the index and proves the criterion. The weight lies in Theorem 5.14 and Lemma 5.18; the rest is the machinery of the method, stated once in general form, and bookkeeping in pair coordinates. From the earlier sections the section uses the index system and its common term z (Proposition 2.11, Lemma 2.15), the ordering of Lemma 2.14, the order-two quotient k_c of Convention 3.1, and the quartic index floor.

5.1 Rickert's approximants and Bennett's criterion

We state the hypergeometric method for arbitrary distinct integer shifts a_0, a_1, a_2; nothing in this subsection involves a Diophantine triple. Rickert's approximants [26] are polynomials p_{ij} of degree at most k whose linear forms $\Lambda_i = \sum_j p_{ij}\vartheta_j$ in the three square roots $\vartheta_j = (1 + a_j x)^{1/2}$ vanish to order $3k$ at $x = 0$, as the proof of Lemma 5.3 shows. Three properties make them usable. Their determinant does not vanish (Lemma 5.3, after Rickert and Bennett), and both this fact and the bounds of Lemma 5.12 rest on one residue representation (Lemma 5.2). Their denominators are controlled: the coefficient products are integers divisible by every prime of the Cipu–Fujita prime product [9] (Lemma 5.5), which exceeds $1.6^k/(4.09 \cdot 10^{13})$ (Lemma 5.6). And Bennett's criterion [6] (Lemma 5.7) turns integer approximants with entries of size P^k and linear forms of size L^{-k} into an approximation measure with exponent $1 + \log P/\log L$.

Convention 5.1. Rickert's approximants ([26], in the normalisation of [10]). Let the **shifts** a_0, a_1, a_2 be distinct integers, $M = \max_l |a_l|$, and

$$F(z) = \prod_{l=0}^{2}(z - a_l), \qquad k_{il} = k + \delta_{il} \quad (0 \le i, l \le 2),$$

where $k \geq 1$ is an integer and δ_{il} the Kronecker delta. For $0 \leq i, j \leq 2$ the **Rickert polynomial** $p_{ij}(x) = p_{ij}^{(k)}(x)$ is

$$p_{ij}(x) = \sum_{h_0+h_1+h_2=k_{ij}-1} \binom{k+\frac{1}{2}}{h_j} x^{h_j}(1+a_j x)^{k-h_j} \prod_{l\neq j} \binom{-k_{il}}{h_l} (a_j - a_l)^{-(k_{il}+h_l)},$$

the sum over all non-negative integers h_0, h_1, h_2 with $h_0 + h_1 + h_2 = k_{ij} - 1$. For a real number x with $|x|M < 1$ the **approximated numbers** are

$$\vartheta_j = \vartheta_j(x) = (1 + a_j x)^{1/2} > 0 \qquad (j = 0, 1, 2),$$

and the **linear forms** are $\Lambda_i(x) = \sum_{j=0}^{2} p_{ij}(x)\vartheta_j(x)$ $(i = 0, 1, 2)$. The index k is suppressed when it is fixed. Throughout, $(1 + zx)^{1/2}$ denotes the principal branch, analytic in the disc $|z| < 1/|x|$.

The **coefficient products** of order k are the rational numbers

$$T_{ij}^{(k)}(h) = 2^{2k-1} \binom{k+\frac{1}{2}}{h_j} \prod_{l\neq j} \binom{-k_{il}}{h_l},$$

for $i, j \in \{0, 1, 2\}$ and every triple $h = (h_0, h_1, h_2)$ of non-negative integers with $h_0 + h_1 + h_2 = k_{ij} - 1$. When all of them are integers, G_k denotes their greatest common divisor.

Lemma 5.2. *Let a_0, a_1, a_2 be distinct integers, let $k \geq 1$ be an integer, and let $p_{ij} = p_{ij}^{(k)}$ be Rickert's polynomials of order k for these shifts, with M, F and k_{il} as in Convention 5.1. Put*

$$g_i(z) = \prod_{l=0}^{2} (z - a_l)^{-k_{il}} = \big((z - a_i)F(z)^k\big)^{-1} \qquad (i = 0, 1, 2).$$

Then for all $0 \leq i, j \leq 2$:

1. *in the ring $\mathbb{Q}[[x]]$ of formal power series, with $\vartheta_j = \sum_{e\geq 0} \binom{1/2}{e} a_j^e x^e$, the coefficient of x^u in $p_{ij}(x)\vartheta_j$ is $\binom{k+1/2}{u} \mathrm{Res}_{z=a_j} z^u g_i(z)$ for every integer $u \geq 0$; in particular $p_{ij}(0) = \mathrm{Res}_{z=a_j} g_i(z)$;*
2. *for every real x with $|x|M < 1$,*

$$p_{ij}(x)\,\vartheta_j(x) = \mathrm{Res}_{z=a_j} \psi_i(z), \qquad \psi_i(z) = (1 + zx)^{k+1/2} g_i(z).$$

Proof. The residue form is Rickert's [26], who defines the approximants by contour integrals and derives the formula of Convention 5.1 from them, and Bennett [6] estimates the approximants through the same integrals; we include a proof for completeness. In view of the formal expansion $(1+zx)^{k+1/2} = \sum_{u\geq 0} \binom{k+1/2}{u} z^u x^u$, item 1 is the formal counterpart of item 2; we prove the two items separately, item 1 in $\mathbb{Q}[[x]]$ and item 2 for real x. For a function ϕ meromorphic near a, $\mathrm{Res}_{z=a}\phi$ is the coefficient of $(z - a)^{-1}$ in its Laurent expansion at a.

We first express the coefficients of p_{ij} by residues. For $e \geq 0$ put $\rho_{ij}(e) = \mathrm{Res}_{z=a_j}(z - a_j)^e g_i(z)$. Since $g_i = (z - a_j)^{-k_{ij}} \prod_{l\neq j}(z - a_l)^{-k_{il}}$ and

$$\prod_{l\neq j} (z - a_l)^{-k_{il}} = \prod_{l\neq j} \sum_{h_l\geq 0} \binom{-k_{il}}{h_l} (a_j - a_l)^{-(k_{il}+h_l)} (z - a_j)^{h_l}$$

near $z = a_j$, we get $\rho_{ij}(e) = \sum \prod_{l\neq j} \binom{-k_{il}}{h_l}(a_j - a_l)^{-(k_{il}+h_l)}$, the sum over $h_l \geq 0$ ($l \neq j$) with $\sum_{l\neq j} h_l = k_{ij} - 1 - e$, for $0 \leq e \leq k_{ij} - 1$, and $\rho_{ij}(e) = 0$ for $e \geq k_{ij}$. Comparing with the formula of Convention 5.1 (with $e = h_j$, and $k_{ij} - 1 \leq k$),

$$p_{ij}(x) = \sum_{e=0}^{k} \binom{k+\frac{1}{2}}{e} \rho_{ij}(e)\, x^e (1 + a_j x)^{k-e}, \qquad p_{ij}(0) = \rho_{ij}(0).$$

We next prove item 1. (For $|x|M < 1$ the series ϑ_j converges to the ϑ_j of Convention 5.1.) For a rational number w put $(1 + a_j x)^w := \sum_e \binom{w}{e} a_j^e x^e$; Vandermonde's identity gives $(1 + a_j x)^w (1 + a_j x)^{w'} = (1 + a_j x)^{w+w'}$, and for $w \in \mathbb{Z}_{\geq 0}$ the series is the polynomial $(1 + a_j x)^w$. Hence $p_{ij}(x)\vartheta_j = \sum_e \binom{k+1/2}{e} \rho_{ij}(e) x^e (1 + a_j x)^{k+1/2-e}$, and its coefficient of x^u ($u \geq 0$) is

$$\begin{aligned} \sum_{e=0}^{u} \binom{k+\frac{1}{2}}{e} \binom{k+\frac{1}{2}-e}{u-e} a_j^{u-e} \rho_{ij}(e) &= \binom{k+\frac{1}{2}}{u} \sum_{e=0}^{u} \binom{u}{e} a_j^{u-e} \rho_{ij}(e) \\ &= \binom{k+\frac{1}{2}}{u} \mathrm{Res}_{z=a_j}\, z^u g_i(z), \end{aligned}$$

using $\binom{w}{e}\binom{w-e}{u-e} = \binom{w}{u}\binom{u}{e}$, $\rho_{ij}(e) = 0$ for $e > k$, and $z^u = \sum_e \binom{u}{e} a_j^{u-e} (z - a_j)^e$. As $\rho_{ij}(0) = \mathrm{Res}_{z=a_j} g_i(z)$, this proves item 1.

We finally prove item 2. Let x be real with $|x|M < 1$, so that ψ_i is analytic in the disc $|z| < 1/|x|$ except for poles at a_0, a_1, a_2. Near a_j, $\psi_i(z) = \chi(z)(z - a_j)^{-k_{ij}}$ with $\chi(z) = (1+zx)^{k+1/2} \prod_{l\neq j} (z - a_l)^{-k_{il}}$ analytic at a_j, so the residue is $\chi^{(e)}(a_j)/e!$, $e = k_{ij} - 1$. By Leibniz's rule, $\chi^{(e)}/e!$ is the sum over $h_j + h_{l_1} + h_{l_2} = e$, where $\{l_1, l_2\} = \{0, 1, 2\} \setminus \{j\}$, of the products of the h-th derivatives divided by $h!$, and $\frac{1}{h!}\frac{d^h}{dz^h}(1 + zx)^{k+1/2} = \binom{k+1/2}{h} x^h (1 + zx)^{k-h} (1 + zx)^{1/2}$, $\frac{1}{h!}\frac{d^h}{dz^h}(z - a_l)^{-k_{il}} = \binom{-k_{il}}{h}(z - a_l)^{-k_{il}-h}$. Evaluating at $z = a_j$ gives exactly $\vartheta_j\, p_{ij}(x)$ by the formula of Convention 5.1. □

Lemma 5.3. *Let a_0, a_1, a_2 be distinct integers, let $k \geq 1$ be an integer, and let $p_{ij}(x)$ be Rickert's polynomials of order k for these shifts (Convention 5.1). Then there is a rational number $C_k \neq 0$ such that*

$$\det\big(p_{ij}(x)\big)_{0\leq i,j\leq 2} = C_k\, x^{3k}.$$

In particular $\det(p_{ij}(x)) \neq 0$ *for every real* $x \neq 0$.

Proof. The nonvanishing of this determinant is due to Rickert [26], and Bennett [5, Section 2] states the identity with an explicit value of C_k, for any number of shifts. We include a proof for completeness. For a rational function $\phi \in \mathbb{Q}(z)$, $\mathrm{Res}_{z=a}\phi$ is the coefficient of $(z - a)^{-1}$ in its Laurent expansion at a, and $[z^{-1}]_\infty \phi$ is the coefficient of z^{-1} in its expansion in powers of $1/z$. We use the residue theorem for rational functions: $\sum_a \mathrm{Res}_{z=a}\phi = [z^{-1}]_\infty \phi$, the sum over the poles a of ϕ; this follows from the partial fraction decomposition, since $[z^{-1}]_\infty (z - a)^{-e}$ is 1 for $e = 1$ and 0 for $e \geq 2$, and polynomials contribute nothing. With F and k_{il} as in Convention 5.1, let

$$g_i(z) = \prod_{l=0}^{2} (z - a_l)^{-k_{il}} = \big((z - a_i)F(z)^k\big)^{-1} \qquad (i = 0, 1, 2)$$

as in Lemma 5.2, and put $\rho_{ij} = \mathrm{Res}_{z=a_j} g_i(z)$. Each p_{ij} is a polynomial in x of degree at most k with rational coefficients, since every term of its defining sum is a rational multiple of $x^{h_j}(1 + a_j x)^{k-h_j}$ with $h_j \leq k_{ij} - 1 \leq k$.

By Lemma 5.2, item 1, $p_{ij}(0) = \rho_{ij}$, and in the ring $\mathbb{Q}[[x]]$ of formal power series, with $\vartheta_j = \sum_{e\ge 0} \binom{1/2}{e} a_j^e x^e$, the coefficient of x^u ($u \ge 0$) in $p_{ij}(x)\vartheta_j$ is $\binom{k+1/2}{u}\mathrm{Res}_{z=a_j} z^u g_i(z)$.

We next show that, in $\mathbb{Q}[[x]]$, $\Lambda_i := \sum_j p_{ij}(x)\vartheta_j \equiv u_k\, x^{3k} \pmod{x^{3k+1}}$ for each i, where $u_k = \binom{k+1/2}{3k}$. Summing these coefficients over j and applying the residue theorem, the coefficient of x^u in Λ_i is $\binom{k+1/2}{u}[z^{-1}]_\infty z^u g_i(z)$. Since $g_i(z) = z^{-3k-1}\prod_l (1-a_l/z)^{-k_{il}} = z^{-3k-1}(1+\sum_{e\ge 1} t_e z^{-e})$ with rational t_e, the expansion of $z^u g_i$ at infinity has only powers $z^{u-3k-1-e}$ ($e \ge 0$), with coefficient 1 for $e = 0$; so $[z^{-1}]_\infty z^u g_i$ is 0 for $u < 3k$ and 1 for $u = 3k$.

We next reduce the determinant to $u_k\mathcal{E}_k$, where $\mathcal{E}_k$ is the determinant of the matrix with rows $(\rho_{i0}, 1, \rho_{i2})$, $i = 0, 1, 2$. Let $\mathbf{p}_0, \mathbf{p}_1, \mathbf{p}_2$ be the columns of $(p_{ij}(x))$ and $\mathcal{E}(x) = \det(p_{ij}(x)) \in \mathbb{Q}[x]$, of degree at most $3k$ because each entry has degree at most k. In $\mathbb{Q}[[x]]$, ϑ_1 is a unit (constant term 1); adding ϑ_0/ϑ_1 times column 0 and ϑ_2/ϑ_1 times column 2 to column 1 does not change the determinant and turns column 1 into $(\Lambda_i/\vartheta_1)_i$. By the previous step $(\Lambda_i)_i = x^{3k}(u_k\mathbf{e} + x\mathbf{g})$ with $\mathbf{e} = (1,1,1)^{\mathsf{T}}$ and $\mathbf{g} \in \mathbb{Q}[[x]]^3$, so

$$\mathcal{E}(x) = \vartheta_1^{-1} x^{3k}\Big(u_k \det\big[\mathbf{p}_0,\, \mathbf{e},\, \mathbf{p}_2\big] + x \det\big[\mathbf{p}_0,\, \mathbf{g},\, \mathbf{p}_2\big]\Big) \equiv u_k\, \mathcal{E}_k\, x^{3k} \pmod{x^{3k+1}},$$

because at $x = 0$ the columns $\mathbf{p}_0, \mathbf{p}_2$ are $(\rho_{i0})_i, (\rho_{i2})_i$ and $\vartheta_1(0) = 1$. As $\deg \mathcal{E} \le 3k$, $\mathcal{E}(x) = u_k\mathcal{E}_k x^{3k}$. Moreover $u_k = \frac{1}{(3k)!}\prod_{e=0}^{3k-1}(k+\frac{1}{2}-e) \ne 0$, since no factor vanishes.

We finally prove $\mathcal{E}_k \ne 0$. Each row of (ρ_{ij}) sums to zero: $\sum_j \rho_{ij} = [z^{-1}]_\infty g_i = 0$, as g_i has order $3k+1 \ge 2$ at infinity. Suppose $\mathcal{E}_k = 0$. Then there is $(\eta_0, \eta_1, \eta_2) \in \mathbb{Q}^3 \setminus \{0\}$ with $\sum_i \eta_i\rho_{i0} = \sum_i \eta_i\rho_{i2} = \sum_i \eta_i = 0$, and by the row sums also $\sum_i \eta_i\rho_{i1} = 0$. Put

$$g(z) = \sum_i \eta_i g_i(z) = \frac{f(z)}{F(z)^{k+1}}, \qquad f(z) = \sum_i \eta_i \prod_{l\ne i}(z - a_l).$$

Then $f(a_i) = \eta_i \prod_{l\ne i}(a_i - a_l)$, so $f \ne 0$; its coefficient of z^2 is $\sum_i \eta_i = 0$, so $\deg f \le 1$; and $\mathrm{Res}_{z=a_j} g = \sum_i \eta_i\rho_{ij} = 0$ for $j = 0, 1, 2$. Since $\deg f < \deg F^{k+1}$, partial fractions give $g = \sum_j \sum_{e=1}^{k+1} \xi_{je}(z-a_j)^{-e}$ with $\xi_{j1} = \mathrm{Res}_{z=a_j} g = 0$. Hence $I = \sum_j \sum_{e=2}^{k+1} \frac{\xi_{je}}{1-e}(z-a_j)^{1-e}$ satisfies $I' = g$, and $J = F^k I$ is a polynomial. At infinity $I = \sum_{e\ge 1} \zeta_e z^{-e}$ and $I' = -\sum_{e\ge 1} e\,\zeta_e z^{-e-1}$, while $g = f/F^{k+1}$ has only powers z^{-e} with $e \ge 3k+3-\deg f \ge 3k+2$; therefore $\zeta_e = 0$ for $e \le 3k$, that is $I = \sum_{e\ge 3k+1} \zeta_e z^{-e}$. As $F^k = z^{3k}(1 + O(z^{-1}))$, the polynomial $J = F^k I$ has only negative powers of z at infinity, so $J = 0$. Then $I = 0$, $g = I' = 0$ and $f = 0$, a contradiction. Hence $\mathcal{E}_k \ne 0$, and $C_k = u_k\mathcal{E}_k \ne 0$. □

Definition 5.4. For an integer $k \ge 1$ the **Cipu–Fujita prime product** $\mathcal{P}(k)$ ([9], proof of Theorem 2.2) is the product of all primes p with

$$p > \sqrt{2k+1}, \qquad \gcd(p, 2k) = 1, \qquad \left\{\frac{k-1}{p}\right\} > \frac{3}{4},$$

where $\{u\} = u - \lfloor u \rfloor$; the empty product is 1.

Lemma 5.5. *Let $k \ge 1$ be an integer, and let $T_{ij}^{(k)}(h)$ be the coefficient products of order k (Convention 5.1).*

1. *For $0 \le h \le k$, $2^{2k-1}\binom{k+1/2}{h} \in \mathbb{Z}$. In particular every $T_{ij}^{(k)}(h)$ is an integer, so G_k is defined.*

2. *Let p be an odd prime with $p \nmid k$ and $\{(k-1)/p\} > \frac{3}{4}$. Then p divides every $T_{ij}^{(k)}(h)$.*

3. $\mathcal{P}(k)$ (Definition 5.4) divides G_k; in particular $G_k \geq \mathcal{P}(k)$.

Proof. Item 1 is a lemma of Rickert [26], as quoted by Cipu, Fujita and Mignotte [10]; items 2 and 3 are the term-wise form of the divisibility used in [9, proof of Theorem 2.2], which cites [5, Lemma 4.1]. We include the proofs. Throughout, v_p denotes the p-adic valuation on $\mathbb{Q}^\times$, and for an integer u and $q \geq 1$ we write $u \bmod q$ for the least non-negative residue.

We first record the valuation of the half-integral binomial coefficients. For $0 \leq h \leq k$,

$$\binom{k+\frac{1}{2}}{h} = \frac{1}{h!}\prod_{e=0}^{h-1}\Big(k+\frac{1}{2}-e\Big) = \frac{\prod_{e=0}^{h-1}(2k+1-2e)}{2^h\, h!},$$

a quotient whose numerator is a product of positive odd integers. Let p be an odd prime and, for $f \geq 1$, let $w_f \in \{0,\dots,p^f-1\}$ be defined by $2w_f \equiv 2k+1 \pmod{p^f}$. Then $p^f \mid 2k+1-2e$ if and only if $e \equiv w_f \pmod{p^f}$, and writing $h = g\,p^f + \eta$ with $0 \leq \eta < p^f$, the interval $0 \leq e \leq h-1$ contains exactly $g + [\eta > w_f]$ such e (here $[\cdot]$ is 1 if the condition holds and 0 otherwise). By Legendre's formula $v_p(h!) = \sum_{f\geq 1}\lfloor h/p^f \rfloor$, so

$$v_p\Big(\binom{k+\frac{1}{2}}{h}\Big) = \sum_{f\geq 1}\big[\,(h \bmod p^f) > w_f\,\big] \;\geq\; \big[\,(h \bmod p) > w_1\,\big] \;\geq 0. \tag{5.1}$$

We next prove item 1. By (5.1), $v_p(2^{2k-1}\binom{k+1/2}{h}) \geq 0$ for every odd prime p. For $p = 2$, the numerator is odd, so $v_2(2^{2k-1}\binom{k+1/2}{h}) = 2k-1-h-v_2(h!)$; this is $2k-1 \geq 1$ if $h = 0$, and for $h \geq 1$ it is at least $2k-1-h-(h-1) = 2(k-h) \geq 0$, since $v_2(h!) = h - (\text{number of binary digits 1 of } h) \leq h-1$. Hence $2^{2k-1}\binom{k+1/2}{h} \in \mathbb{Z}$. In $T_{ij}^{(k)}(h)$ one has $h_j \leq k_{ij}-1 \leq k$, and $\binom{-v}{h_l} = (-1)^{h_l}\binom{v+h_l-1}{h_l} \in \mathbb{Z}$ for every integer $v \geq 1$; so $T_{ij}^{(k)}(h) \in \mathbb{Z}$.

We next record the valuation of the ordinary factors. For integers $v \geq 1$ and $h \geq 0$, $\binom{-v}{h} = (-1)^h\binom{v+h-1}{h}$, and by Legendre's formula

$$v_p\Big(\binom{v+h-1}{h}\Big) = \sum_{f\geq 1}\Big(\Big\lfloor\frac{v-1+h}{p^f}\Big\rfloor - \Big\lfloor\frac{v-1}{p^f}\Big\rfloor - \Big\lfloor\frac{h}{p^f}\Big\rfloor\Big).$$

Each summand is ≥ 0, and the summand $f=1$ equals $\big[(v-1) \bmod p + h \bmod p \geq p\big]$. Hence

$$v_p\Big(\binom{-v}{h}\Big) \;\geq\; \big[\,((v-1) \bmod p) + (h \bmod p) \geq p\,\big] \;\geq 0. \tag{5.2}$$

We now prove item 2. Put $\rho = (k-1) \bmod p$, so that $\{(k-1)/p\} = \rho/p$ and the hypothesis reads $4\rho > 3p$. Since $p \nmid k$, $\rho \neq p-1$, so $\rho \leq p-2$ and $k \bmod p = \rho+1$. Since $2k+1 = 2(k-1)+3 \equiv 2\rho+3 \pmod p$ and $\frac{3}{2}p < 2\rho \leq 2p-4$, the integer $2\rho+3-p$ is even (as p is odd) and lies in $[1, p-1]$, so

$$w_1 = \frac{2\rho+3-p}{2} = \rho - \frac{p-3}{2}.$$

Fix i,j and $h = (h_0,h_1,h_2)$ with $h_0+h_1+h_2 = k_{ij}-1$, and write $\bar{h}_l = h_l \bmod p$. Since p is odd, $v_p(T_{ij}^{(k)}(h)) = v_p(\binom{k+1/2}{h_j}) + \sum_{l\neq j} v_p(\binom{-k_{il}}{h_l})$, a sum of non-negative terms by (5.1) and (5.2). Suppose that $p \nmid T_{ij}^{(k)}(h)$, that is $v_p(T_{ij}^{(k)}(h)) = 0$. Then (5.1) gives $\bar{h}_j \leq w_1$. For $l \neq j$, $k_{il}-1 \in \{k-1, k\}$, so $(k_{il}-1) \bmod p \in \{\rho, \rho+1\}$ is at least ρ, and (5.2) gives $\bar{h}_l \leq p-1-\rho$. Therefore

$$0 \leq \bar{h}_0+\bar{h}_1+\bar{h}_2 \leq w_1 + 2(p-1-\rho) = \frac{3p-1}{2} - \rho < \rho,$$

where the last inequality is $3p-1<4\rho$. On the other hand $\bar h_0+\bar h_1+\bar h_2\equiv h_0+h_1+h_2=k_{ij}-1 \pmod p$, and $k_{ij}-1\in\{k-1,k\}$ is congruent to ρ or to $\rho+1$, both in $[0,p-1]$. As $0\le \bar h_0+\bar h_1+\bar h_2<\rho\le p-2$, the sum $\bar h_0+\bar h_1+\bar h_2$ is its own least residue and would equal ρ or $\rho+1$, which is impossible. Hence $p\mid T_{ij}^{(k)}(h)$.

We finally prove item 3. A prime p counted in $\mathcal P(k)$ satisfies $p<\frac43(k-1)$: this is clear if $p\le k-1$ (then $k\ge 2$), and if $p>k-1$ then $\{(k-1)/p\}=(k-1)/p>\frac34$. So $\mathcal P(k)$ is a finite product of distinct primes. Every such prime satisfies $\gcd(p,2k)=1$, so it is odd and does not divide k, and it satisfies $\{(k-1)/p\}>\frac34$; by item 2 it divides every $T_{ij}^{(k)}(h)$. Hence $\mathcal P(k)$ divides every $T_{ij}^{(k)}(h)$, hence their greatest common divisor G_k, which is positive; so $G_k\ge\mathcal P(k)$.

□

Lemma 5.6. *For every integer $k\ge 1$,*

$$\mathcal P(k)>\frac{1.6^k}{4.09\cdot 10^{13}},$$

where $\mathcal P(k)$ is the Cipu–Fujita prime product (Definition 5.4).

Proof. This is proved in [9], proof of Theorem 2.2. With $J_l(k)$ the open interval $\big((k-1)/l,\,4(k-1)/(4l-1)\big)$, display (2.1) there bounds $\mathcal P(k)$ from below by the product of the primes $p\in J_l(k)$ with $\gcd(p,2k)=1$, over $1\le l\le\lfloor(k-1)/\sqrt{2k-1}\rfloor$. The logarithm of this product is shown there to exceed $0.4706\,k>k\log 1.6$ for $k\ge 903683$ (explicit prime-number estimates, applied to the intervals with $l\le 13$), and to exceed $k\log 1.6-31.342$ for $1\le k\le 903682$ (computer search; the minimum is attained at $k=607$). Since $e^{31.342}<4.09\cdot 10^{13}$, this gives the claim; display (2.2) there states the resulting bound for an integer that is a multiple of $\mathcal P(k)$, but both derivations bound the right side of (2.1), hence $\mathcal P(k)$.

□

Lemma 5.7. *Let θ_1,θ_2 be real numbers and $\theta_0=1$. Assume that there are positive real numbers ℓ_*,p_*,L,P with $L>1$ such that for every positive integer k there are integers p_{ijk} $(0\le i,j\le 2)$ with $\det(p_{ijk})_{0\le i,j\le 2}\ne 0$,*

$$|p_{ijk}|\le p_*P^k\quad(0\le i,j\le 2),\qquad\Big|\sum_{j=0}^{2}p_{ijk}\theta_j\Big|\le\ell_*L^{-k}\quad(0\le i\le 2).$$

Then for all integers A_0,A_1,A_2 with $A_0>0$,

$$\max\Big\{\Big|\theta_1-\frac{A_1}{A_0}\Big|,\Big|\theta_2-\frac{A_2}{A_0}\Big|\Big\}>C\,A_0^{-\tau},\qquad\tau=1+\frac{\log P}{\log L},\qquad C^{-1}=4p_*P\left(\max\{1,2\ell_*\}\right)^{\tau-1}.$$

Proof. This is Bennett's criterion [6], as stated by Cipu, Fujita and Mignotte [10]; the constants p,l, the exponent λ, the numerators p_1,p_2 and the denominator q of the sources are written p_*,ℓ_*, τ, A_1,A_2 and A_0 here. The statement is invariant under a permutation of the index j, since only the set of columns and the linear forms enter; this is used when the columns are indexed by shifts a_0,a_1,a_2 of Convention 5.1 with $a_1=0$, so that the approximated number $\vartheta_1=1$ stands in the middle column. □

5.2 An approximation measure for a pair representation

We now place an Euler triple in this setting. A pair representation factors the two smaller elements so that the cross products are $p_1q_2 = r+\sigma$ and $p_2q_1 = r-\sigma$, and the sums $p_3 = p_1+p_2$ and $q_3 = q_1+q_2$ factor the largest, $c = p_3q_3$; every Euler triple has one of sign $+1$, its canonical quadruple (Lemma 5.10).

Definition 5.8. Let $\{a,b,c\}$ be an Euler triple with root r (Definition 2.3). A **pair representation** of $\{a,b,c\}$ of **sign** $\sigma \in \{-1,1\}$ is a quadruple (p_1,q_1,p_2,q_2) of positive integers with

$$a = p_1q_1, \qquad b = p_2q_2, \qquad p_1q_2 - p_2q_1 = 2\sigma.$$

The **canonical quadruple** of $\{a,b,c\}$ is the quadruple of rational numbers

$$p_1 = \gcd(a, r+1), \qquad q_1 = \frac{a}{p_1}, \qquad q_2 = \frac{r+1}{p_1}, \qquad p_2 = \frac{r-1}{q_1}.$$

The **pair coordinates** of a pair representation are the vectors

$$(p_1,q_1), \qquad (p_2,q_2), \qquad (p_3,q_3) = (p_1+p_2,\ q_1+q_2).$$

Definition 5.9. Let (p_1,q_1,p_2,q_2) be a pair representation of sign σ of an Euler triple $\{a,b,c\}$, with $p_3 = p_1+p_2$ and $q_3 = q_1+q_2$ (Definition 5.8). Its **hypergeometric parameter** and its **shifts** are

$$N = \tfrac{1}{2}\,p_1p_2q_3, \qquad a_0 = -\sigma p_2, \qquad a_1 = 0, \qquad a_2 = \sigma p_1,$$

and its **rescaled roots** are the positive real numbers

$$\theta_1 = \frac{p_3}{p_1}\sqrt{\frac{a}{c}}, \qquad \theta_2 = \frac{p_3}{p_2}\sqrt{\frac{b}{c}}.$$

These data are chosen so that the rescaled roots are numbers that Rickert's approximants approximate. By item 3 of the next lemma, $\theta_1 = \sqrt{1+a_0/N}$ and $\theta_2 = \sqrt{1+a_2/N}$, while $\sqrt{1+a_1/N} = 1$; so $(\theta_1,1,\theta_2)$ are the approximated numbers $\vartheta_0,\vartheta_1,\vartheta_2$ of Convention 5.1 at $x = 1/N$. The same item gives $2(N+a_j)/\Delta_j = q_1, -q_3, q_2$ for $j = 0,1,2$, which is the hypothesis under which Lemma 5.11 makes the scaled approximants integers.

Lemma 5.10. *Let $\{a,b,c\}$ be an Euler triple with roots r,s,t (Definition 2.3), and use the notation of Definition 5.8 and Definition 5.9.*

1. *The canonical quadruple of $\{a,b,c\}$ is a pair representation of sign $+1$. Every pair representation of sign σ satisfies*

$$p_1q_2 = r+\sigma, \qquad p_2q_1 = r-\sigma.$$

2. *For every pair representation of sign σ,*

$$c = p_3q_3, \qquad s = p_1q_3 - \sigma = p_3q_1 + \sigma, \qquad t = p_3q_2 - \sigma = p_2q_3 + \sigma.$$

3. *For every pair representation of sign σ, the hypergeometric parameter N is a positive integer and*

$$N + a_0 = \tfrac{1}{2}\, p_2 p_3 q_1, \qquad N + a_1 = \tfrac{1}{2}\, p_1 p_2 q_3, \qquad N + a_2 = \tfrac{1}{2}\, p_1 p_3 q_2;$$

moreover, with $\Delta_j = \prod_{l \neq j}(a_j - a_l)$, one has $\Delta_0 = p_2 p_3$, $\Delta_1 = -p_1 p_2$, $\Delta_2 = p_1 p_3$, so that

$$\frac{2(N + a_0)}{\Delta_0} = q_1, \qquad \frac{2(N + a_1)}{\Delta_1} = -q_3, \qquad \frac{2(N + a_2)}{\Delta_2} = q_2.$$

Consequently

$$\theta_1 = \sqrt{1 + \frac{a_0}{N}}, \qquad \theta_2 = \sqrt{1 + \frac{a_2}{N}}, \qquad \frac{c}{a} = \frac{p_3^2}{p_1^2} \cdot \frac{p_1 q_3}{p_1 q_3 - 2\sigma}.$$

4. *For every pair representation of sign σ, $p_1 \leq p_2$ and $q_1 \leq q_2$.*

Proof. We first prove item 1. By Definition 2.3 and item 4 of Lemma 2.4, $a \geq 1$ and $b \geq 3$, so $r^2 = ab + 1 \geq 4$ and $r \geq 2$. Put $p_1 = \gcd(a, r+1)$, $q_1 = a/p_1$, $q_2 = (r+1)/p_1$; these are positive integers with $\gcd(q_1, q_2) = 1$. From $ab = r^2 - 1 = (r-1)(r+1)$ we get $p_1 q_1 b = (r-1) p_1 q_2$, hence $q_1 b = (r-1) q_2$, and $\gcd(q_1, q_2) = 1$ gives $q_1 \mid r - 1$. Thus $p_2 = (r-1)/q_1$ is a positive integer, $b = (r-1)q_2/q_1 = p_2 q_2$, and $p_1 q_2 - p_2 q_1 = (r+1) - (r-1) = 2$. So the canonical quadruple is a pair representation of sign $+1$. Finally let (p_1, q_1, p_2, q_2) have sign σ and put $u = p_1 q_2$, $v = p_2 q_1$. Then $u, v > 0$, $uv = ab = r^2 - 1$ and $u - v = 2\sigma$, so $(u+v)^2 = (u-v)^2 + 4uv = 4r^2$, $u + v = 2r$, and $u = r + \sigma$, $v = r - \sigma$.

We next prove item 2. By Definition 2.3, $c = a + b + 2r$, $s = a + r$ and $t = b + r$. By item 1, $p_3 q_3 = (p_1 + p_2)(q_1 + q_2) = a + b + p_1 q_2 + p_2 q_1 = a + b + 2r = c$, $p_1 q_3 - \sigma = a + (r + \sigma) - \sigma = s$, $p_3 q_1 + \sigma = a + (r - \sigma) + \sigma = s$, $p_3 q_2 - \sigma = (r + \sigma) + b - \sigma = t$ and $p_2 q_3 + \sigma = (r - \sigma) + b + \sigma = t$.

We now prove item 3. We show that N is an integer. Since $p_1 q_2 - p_2 q_1 = 2\sigma$ is even, $p_1 q_2 \equiv p_2 q_1 \pmod 2$. If $p_1 p_2$ is even, $p_1 p_2 q_3$ is even. If p_1 and p_2 are both odd, then $q_1 \equiv q_2 \pmod 2$, so $q_3 = q_1 + q_2$ is even. In both cases $N = \frac{1}{2} p_1 p_2 q_3 \in \mathbb{Z}$, and $N > 0$. Using $p_1 q_2 - 2\sigma = p_2 q_1$ and $p_2 q_1 + 2\sigma = p_1 q_2$ from item 1,

$$N - \sigma p_2 = \tfrac{1}{2} p_2 \,(p_1 q_1 + p_1 q_2 - 2\sigma) = \tfrac{1}{2} p_2 \,(p_1 q_1 + p_2 q_1) = \tfrac{1}{2} p_2 p_3 q_1,$$

$$N + \sigma p_1 = \tfrac{1}{2} p_1 \,(p_2 q_1 + p_2 q_2 + 2\sigma) = \tfrac{1}{2} p_1 \,(p_1 q_2 + p_2 q_2) = \tfrac{1}{2} p_1 p_3 q_2.$$

The shift differences are $a_0 - a_1 = -\sigma p_2$, $a_0 - a_2 = -\sigma p_3$, $a_1 - a_2 = -\sigma p_1$, so $\Delta_0 = (-\sigma p_2)(-\sigma p_3) = p_2 p_3$, $\Delta_1 = (\sigma p_2)(-\sigma p_1) = -p_1 p_2$, $\Delta_2 = (\sigma p_3)(\sigma p_1) = p_1 p_3$, and the three quotients are q_1, $-q_3$, q_2. Using $a = p_1 q_1$, $b = p_2 q_2$ and $c = p_3 q_3$ (item 2),

$$\theta_1^2 = \frac{p_3^2}{p_1^2} \cdot \frac{p_1 q_1}{p_3 q_3} = \frac{p_2 p_3 q_1}{p_1 p_2 q_3} = \frac{N + a_0}{N}, \qquad \theta_2^2 = \frac{p_3^2}{p_2^2} \cdot \frac{p_2 q_2}{p_3 q_3} = \frac{p_1 p_3 q_2}{p_1 p_2 q_3} = \frac{N + a_2}{N},$$

and $\theta_1, \theta_2 > 0$, which gives the two square roots. Finally $p_3 q_1 = p_1 q_3 - 2\sigma$ by item 2, so $c/a = p_3 q_3/(p_1 q_1) = p_3^2 q_3/(p_1(p_1 q_3 - 2\sigma))$.

We finally prove item 4. From item 1, $\frac{p_1}{p_2} \cdot \frac{q_2}{q_1} = \frac{r+\sigma}{r-\sigma}$ and $\frac{p_1}{p_2} \cdot \frac{q_1}{q_2} = \frac{a}{b}$, whence

$$\frac{p_1^2}{p_2^2} = \frac{a(r+\sigma)}{b(r-\sigma)}, \qquad \frac{q_1^2}{q_2^2} = \frac{a(r-\sigma)}{b(r+\sigma)}.$$

By Lemma 2.4, item 4, $b-a \geq 2$. Now $a(r+1) \leq b(r-1)$ is equivalent to $a+b \leq r(b-a)$, which holds because both sides are positive and $r^2(b-a)^2 - (a+b)^2 = (ab+1)(b-a)^2 - (a+b)^2 = ab\big((b-a)^2-4\big) \geq 0$. Also $a(r-1) < b(r+1)$, as $a < b$. For $\sigma = 1$ this gives $p_1 \leq p_2$ and $q_1 < q_2$; for $\sigma = -1$ it gives $p_1 < p_2$ and $q_1 \leq q_2$.

□

Lemma 5.11. *Let a_0, a_1, a_2 be distinct integers, let $k \geq 1$, and let $p_{ij} = p_{ij}^{(k)}$ and G_k be as in Convention 5.1. Let N be a nonzero rational number with $N + a_j \neq 0$ $(j = 0, 1, 2)$, put $\Delta_j = \prod_{l \neq j}(a_j - a_l)$ and $\Delta = |(a_0 - a_1)(a_0 - a_2)(a_1 - a_2)|$, and assume that*

$$\frac{2(N + a_j)}{\Delta_j} \in \mathbb{Z} \qquad (j = 0, 1, 2).$$

Then for all $i, j \in \{0, 1, 2\}$,

$$\hat{p}_{ij} := \frac{(8\Delta N)^k}{2\,G_k}\, p_{ij}\left(\frac{1}{N}\right) \in \mathbb{Z}.$$

In particular, if N and a_0, a_1, a_2 are the hypergeometric parameter and the shifts of a pair representation of an Euler triple (Definition 5.9), the hypothesis holds and $\Delta = p_1 p_2 p_3$, so that

$$\frac{(8\,p_1p_2p_3N)^k}{2\,G_k}\, p_{ij}\left(\frac{1}{N}\right) \in \mathbb{Z} \qquad (k \geq 1,\ 0 \leq i, j \leq 2).$$

Proof. By Lemma 5.5, item 1, the coefficient products $T_{ij}^{(k)}(h)$ are integers, so G_k is defined. Write $Y_j = 2(N + a_j)/\Delta_j \in \mathbb{Z}$.

We first establish the closed form of a single term. Fix i, j and $h = (h_0, h_1, h_2)$ with $h_0 + h_1 + h_2 = k_{ij} - 1$, and write $\{l_1, l_2\} = \{0, 1, 2\} \setminus \{j\}$. Since $(1 + a_j/N)^{k-h_j} N^{-h_j} = (N + a_j)^{k-h_j} N^{-k}$ and $\Delta^k = \pm(a_{l_1} - a_{l_2})^k \prod_{l \neq j}(a_j - a_l)^k$,

$$2^k \Delta^k N^k \cdot \frac{(1 + a_j/N)^{k-h_j} N^{-h_j}}{\prod_{l \neq j}(a_j - a_l)^{k_{il}+h_l}} = \pm\, 2^k\, (N + a_j)^{k-h_j}\, (a_{l_1} - a_{l_2})^k \prod_{l \neq j} (a_j - a_l)^{\,k-k_{il}-h_l}.$$

By hypothesis $2(N + a_j) = Y_j \Delta_j = Y_j \prod_{l \neq j}(a_j - a_l)$, so $2^k (N + a_j)^{k-h_j} = 2^{h_j} Y_j^{k-h_j} \prod_{l \neq j}(a_j - a_l)^{k-h_j}$, and collecting the exponents of $a_j - a_l$ gives

$$2^k \Delta^k N^k \cdot \frac{(1 + a_j/N)^{k-h_j} N^{-h_j}}{\prod_{l \neq j}(a_j - a_l)^{k_{il}+h_l}} = \pm\, 2^{h_j}\, Y_j^{\,k-h_j}\, (a_{l_1} - a_{l_2})^k \prod_{l \neq j} (a_j - a_l)^{\,k-h_j-h_l-\delta_{il}}.$$

We next show that the right side is an integer. Since $h_j + h_l = k_{ij} - 1 - h_{l'}$ for the third index l', we have $k - h_j - h_l - \delta_{il} = k - k_{ij} + 1 + h_{l'} - \delta_{il} = 1 - \delta_{ij} - \delta_{il} + h_{l'} \geq 0$, because $j \neq l$ so at most one of δ_{ij}, δ_{il} equals 1. Also $k - h_j \geq k - (k_{ij} - 1) \geq 0$. Hence every factor on the right is an integer.

We now prove the integrality of $\hat{p}_{ij}$. Multiplying the formula of Convention 5.1 for $p_{ij}(1/N)$ by $2^{3k-1}\Delta^k N^k = 2^{2k-1} \cdot 2^k \Delta^k N^k$ gives

$$2^{3k-1}\Delta^k N^k\, p_{ij}(1/N) = \sum_h T_{ij}^{(k)}(h) \cdot \Big[2^k \Delta^k N^k \frac{(1 + a_j/N)^{k-h_j} N^{-h_j}}{\prod_{l \neq j}(a_j - a_l)^{k_{il}+h_l}}\Big].$$

In each summand $T_{ij}^{(k)}(h)$ is an integer divisible by G_k, and the bracket is an integer by the first two steps. Hence the sum is an integer divisible by G_k, and $\hat{p}_{ij} = 2^{3k-1}\Delta^k N^k p_{ij}(1/N)/G_k \in \mathbb{Z}$, as $(8\Delta N)^k/2 = 2^{3k-1}\Delta^k N^k$.

Finally we verify the hypothesis for a pair representation. By Lemma 5.10, item 3, N is a positive integer, $\Delta_0 = p_2p_3$, $\Delta_1 = -p_1p_2$, $\Delta_2 = p_1p_3$, and $2(N+a_j)/\Delta_j$ equals q_1, $-q_3$, q_2 for $j = 0, 1, 2$, which are integers; moreover $N + a_0 = \frac{1}{2}p_2p_3q_1$, $N + a_1 = N$ and $N + a_2 = \frac{1}{2}p_1p_3q_2$ are positive, and the shifts $-\sigma p_2, 0, \sigma p_1$ are distinct as $p_1, p_2 > 0$. So the hypothesis holds, and $\Delta = |\Delta_0\Delta_1\Delta_2|^{1/2} = p_1p_2p_3$.

□

Lemma 5.12. *Let (p_1, q_1, p_2, q_2) be a pair representation of an Euler triple, with hypergeometric parameter N, shifts a_0, a_1, a_2 and rescaled roots θ_1, θ_2 (Definition 5.9), and assume $N \geq 3p_2$. Put $\mu = p_2/N \leq \frac{1}{3}$, and let $p_{ij} = p_{ij}^{(k)}$, ϑ_j, Λ_i be Rickert's approximants (Convention 5.1) for these shifts at $x = 1/N$. Then $(\vartheta_0, \vartheta_1, \vartheta_2) = (\theta_1, 1, \theta_2)$, and for every integer $k \geq 1$ and all $0 \leq i, j \leq 2$:*

1. $\Big|\Lambda_i\Big(\dfrac{1}{N}\Big)\Big| \leq \dfrac{27}{64}\,(1-\mu)^{-1}\Big\{\dfrac{27}{4}(1-\mu)^2N^3\Big\}^{-k}$;
2. $\Big|p_{ij}\Big(\dfrac{1}{N}\Big)\Big| \leq \Big(\dfrac{1+\frac{3}{2}\mu}{1-\mu}\Big)^{1/2}\Big(\dfrac{4}{p_1^2p_2}\Big)^k$.

Proof. The two bounds are those of Cipu, Fujita and Mignotte [10], which follow the arguments of Bennett [6], except that the prefactor in item 2 is taken here for both signs of the representation and for the shift a_0, whereas the source gives its value for $a_2 > 0$ only; we give the proof. Throughout, $x = 1/N$, σ is the sign of the representation and $M = \max_l |a_l| = p_2$, since $p_1 \leq p_2$ (Lemma 5.10, item 4); so $xM = \mu < 1$. By Lemma 5.10, item 3, $\vartheta_0 = (1 + a_0/N)^{1/2} = \theta_1$ and $\vartheta_2 = (1 + a_2/N)^{1/2} = \theta_2$, and $\vartheta_1 = 1$ as $a_1 = 0$. Put

$$\psi_i(z) = (1+zx)^{k+1/2}\,(z-a_i)^{-1}F(z)^{-k}, \qquad F(z) = \prod_l (z - a_l),$$

which is analytic in $|z| < N$ except for poles at a_0, a_1, a_2.

We first note that $p_{ij}(x)\vartheta_j$ is the residue of ψ_i at a_j, by Lemma 5.2, item 2 (there $\psi_i = (1+zx)^{k+1/2}g_i$ with $g_i = \big((z-a_i)F^k\big)^{-1}$, and $|x|M = \mu < 1$), so that, by the residue theorem, $\Lambda_i(x) = \frac{1}{2\pi\sqrt{-1}}\oint \psi_i(z)\,dz$ over the counter-clockwise circle $|z| = T$, for any $M < T < N$.

We next prove item 1. The integrand ψ_i extends analytically to $\mathbb{C}\setminus\big((-\infty, -N]\cup\{a_0, a_1, a_2\}\big)$, with $|\psi_i(z)| = O(|z|^{-2k-1/2})$ at infinity, so the circle of radius $T \to \infty$ contributes nothing and the contour can be collapsed onto the cut: $\oint \psi_i\,dz = \int_{-\infty}^{-N}\big(\psi_i^+(z) - \psi_i^-(z)\big)dz$, where $\psi_i^\pm$ are the boundary values from the upper and lower half-planes (the small circle around the branch point $-N$ contributes nothing, as ψ_i is bounded there). For $z = -\xi$, $\xi > N$, one has $(1+zx)^{1/2} = \pm\sqrt{-1}\,(\xi/N - 1)^{1/2}$ from above and below, so $\psi_i^+(-\xi) - \psi_i^-(-\xi) = 2\sqrt{-1}\,(1 - \xi/N)^k(\xi/N-1)^{1/2}\big/\big((-\xi - a_i)F(-\xi)^k\big)$. Since $|\xi + a_l| \geq \xi - M$ for all l and $\xi \geq N > M$,

$$\begin{aligned}|\Lambda_i(x)| &\leq \frac{1}{\pi}\int_N^\infty \frac{(\xi/N-1)^{k+1/2}}{(\xi - M)^{3k+1}}\,d\xi = \frac{N^{-3k}}{\pi}\int_0^\infty \frac{v^{k+1/2}\,dv}{(v+1-\mu)^{3k+1}} \\ &= \frac{N^{-3k}(1-\mu)^{-2k+1/2}}{\pi}\,\mathrm{B}\Big(k+\frac{3}{2},\, 2k-\frac{1}{2}\Big),\end{aligned}$$

by the substitutions $\xi = N(1+v)$, $v = (1-\mu)w$ and $\int_0^\infty w^{u_1-1}(1+w)^{-u_1-u_2}dw = \mathrm{B}(u_1,u_2)$. We claim $\mathrm{B}(k+\frac{3}{2},2k-\frac{1}{2}) \le \frac{27\pi}{64}(\frac{4}{27})^k$ for $k \ge 1$. At $k=1$, $\mathrm{B}(\frac{5}{2},\frac{3}{2}) = \Gamma(\frac{5}{2})\Gamma(\frac{3}{2})/\Gamma(4) = \frac{\pi}{16}$, with equality. The ratio of consecutive values is

$$\frac{\mathrm{B}(k+\frac{5}{2},2k+\frac{3}{2})}{\mathrm{B}(k+\frac{3}{2},2k-\frac{1}{2})} = \frac{(k+\frac{3}{2})(2k+\frac{1}{2})(2k-\frac{1}{2})}{(3k+3)(3k+2)(3k+1)} < \frac{4}{27},$$

because $4(3k+3)(3k+2)(3k+1) - 27(k+\frac{3}{2})(2k+\frac{1}{2})(2k-\frac{1}{2}) = 54k^2 + \frac{555}{4}k + \frac{273}{8} > 0$. Hence, as $(1-\mu)^{3/2} \le 1$,

$$|\Lambda_i(x)| \le \frac{27}{64}(1-\mu)^{-2k-1}\Big(\frac{4}{27}\Big)^k N^{-3k} = \frac{27}{64}(1-\mu)^{-1}\Big\{\frac{27}{4}(1-\mu)^2N^3\Big\}^{-k}.$$

We now prove item 2. Fix j and let Γ_j be the circle $|z-a_j| = \rho$, $\rho = p_1/2$. It separates a_j from the other shifts (their distances to a_j are among p_1, p_2, p_3, all $\ge 2\rho$), and lies in $|z| \le p_2 + p_1/2 < N$. By the residue representation, $|p_{ij}(x)|\,\vartheta_j \le \rho \cdot \max_{\Gamma_j}|1+zx|^{k+1/2}\big/\big(\min_{\Gamma_j}|z-a_i| \cdot \min_{\Gamma_j}|F(z)|^k\big)$, and $\min_{\Gamma_j}|z-a_i| \ge \rho$ (equality if $i=j$; otherwise $|z-a_i| \ge |a_j-a_i| - \rho \ge p_1 - \rho = \rho$). Also $\max_{\Gamma_j}|1+zx| \le 1 + (|a_j|+\rho)/N =: \Upsilon_j$. For $Z_j := \min_{\Gamma_j}|F(z)|$, write $z = a_j + \rho e^{\sqrt{-1}\phi}$; the two factors $|z-a_l|$, $l \ne j$, are $\big(X_l^2 + \rho^2 + 2\varepsilon_l X_l \rho\cos\phi\big)^{1/2}$ with $X_l = |a_j - a_l|$ and $\varepsilon_l = \mathrm{sgn}(a_j - a_l)$. For $j=0$ and $j=2$ the two signs ε_l coincide (a_0 and a_2 are the extreme shifts), so both factors are minimal at the same ϕ, giving $Z_0 = \rho(p_2-\rho)(p_3-\rho)$ and $Z_2 = \rho(p_1-\rho)(p_3-\rho)$. For $j=1$ the signs differ and the product of the squared factors is $(p_1^2+\rho^2-2p_1\rho u)(p_2^2+\rho^2+2p_2\rho u)$, $u = \cos\phi \in [-1,1]$, a concave quadratic in u, minimal at an endpoint; the values there are $(p_1-\rho)^2(p_2+\rho)^2$ and $(p_1+\rho)^2(p_2-\rho)^2$, and the first is the smaller since $(p_1+\rho)(p_2-\rho) - (p_1-\rho)(p_2+\rho) = 2\rho(p_2-p_1) \ge 0$. So $Z_1 = \rho(p_1-\rho)(p_2+\rho)$. With $\rho = p_1/2$:

$$Z_1 = Z_2 = \frac{p_1^2(p_1+2p_2)}{8}, \qquad Z_0 = \frac{p_1(2p_2-p_1)(2p_2+p_1)}{8},$$

$$\Upsilon_1 = 1 + \frac{p_1}{2N}, \qquad \Upsilon_2 = 1 + \frac{3p_1}{2N}, \qquad \Upsilon_0 = 1 + \frac{2p_2+p_1}{2N}.$$

Hence $|p_{ij}(x)| \le (\Upsilon_j/\vartheta_j^2)^{1/2}(\Upsilon_j/Z_j)^k$. For $j=1,2$, $\Upsilon_j \le 1 + \frac{3p_1}{2N}$ and $\Upsilon_j/Z_j \le \frac{8(1+3p_1/(2N))}{p_1^2(p_1+2p_2)}$. For $j=0$ the same bound holds because

$$\begin{aligned}\frac{\Upsilon_0}{Z_0} \le \frac{8(1+\frac{3p_1}{2N})}{p_1^2(p_1+2p_2)} &\iff p_1\Big(1+\frac{2p_2+p_1}{2N}\Big) \le (2p_2-p_1)\Big(1+\frac{3p_1}{2N}\Big)\\ &\iff -2(p_2-p_1)\Big(1+\frac{p_1}{N}\Big) \le 0.\end{aligned}$$

The prefactors: $\vartheta_1 = 1$, $\vartheta_2^2 = 1 + \sigma p_1/N \ge 1 - p_1/N$, $\vartheta_0^2 = 1 - \sigma p_2/N \ge 1-\mu$, so $\Upsilon_j/\vartheta_j^2 \le \frac{1+3p_1/(2N)}{1-p_1/N} \le \frac{1+\frac{3}{2}\mu}{1-\mu}$ for $j=1,2$ (the function $y \mapsto (1+\frac{3}{2}y)/(1-y)$ is increasing and $p_1/N \le \mu$) and $\Upsilon_0/\vartheta_0^2 \le \frac{1+\frac{3}{2}\mu}{1-\mu}$ since $2p_2+p_1 \le 3p_2$. Hence

$$\Big|p_{ij}\Big(\frac{1}{N}\Big)\Big| \le \Big(\frac{1+\frac{3}{2}\mu}{1-\mu}\Big)^{1/2}\Big(\frac{8\,(1+\frac{3p_1}{2N})}{p_1^2\,(p_1+2p_2)}\Big)^k.$$

Finally $N \ge 3p_2$ gives $8(1+\frac{3p_1}{2N})p_2 \le 4(p_1+2p_2)$, which is equivalent to $\frac{3p_1p_2}{N} \le p_1$; this is item 2.

□

Convention 5.13. The **measure constant** of the hypergeometric method is $\omega = 1.3175$.

The value of ω is fitted to the hypothesis $p_1 q_3 \geq 168$ of the next theorem. For a pair representation the ratio $\mu = p_2/N$ of Lemma 5.12 equals $2/(p_1 q_3)$, so this hypothesis reads $\mu \leq \frac{1}{84}$. The linear forms of the scaled approximants decay like L_0^{-k} with $L_0 = 1.35(1-\mu)^2 N^2/\Delta$, where $\Delta = p_1 p_2 p_3$ and $1.35 = \frac{27}{20}$ is the factor $\frac{27}{4}$ of Lemma 5.12 divided by the factor $8/1.6 = 5$ that the scaling of Lemma 5.11 leaves after the bound for the prime product. The constant ω lies just below $1.35(1 - \frac{1}{84})^2 = 1.3180\ldots$, so for every such representation L_0 may be replaced by $\omega N^2/\Delta$, the quantity in the denominator of the exponent τ.

Theorem 5.14. *Let (p_1, q_1, p_2, q_2) be a pair representation of an Euler triple, with hypergeometric parameter N and rescaled roots θ_1, θ_2 (Definition 5.9), and assume that $p_1 q_3 \geq 168$. With ω as in Convention 5.13, put*

$$\tau = 1 + \frac{\log\bigl(20\, p_3 N/p_1\bigr)}{\log\bigl(\omega N^2/(p_1 p_2 p_3)\bigr)} = 1 + \frac{\log\bigl(10\, p_2 p_3 q_3\bigr)}{\log\bigl(\omega\, p_1 p_2 q_3^2/(4p_3)\bigr)}.$$

Then $\tau < 2$ if and only if $40\, p_3^2 < \omega\, p_1 q_3$, and in that case, for all integers A_0, A_1, A_2 with $A_0 > 0$,

$$\max\Bigl\{\Bigl|\theta_1 - \frac{A_1}{A_0}\Bigr|, \Bigl|\theta_2 - \frac{A_2}{A_0}\Bigr|\Bigr\} > \Bigl(2.9 \cdot 10^{28}\, \frac{p_3}{p_1}\, N\Bigr)^{-1} A_0^{-\tau}.$$

Proof. We apply Bennett's criterion (Lemma 5.7) to Rickert's approximants at $x = 1/N$, scaled to integers. Their entries grow at most like P^k and their linear forms decay at least like L^{-k}, where $P = 20 p_3 N/p_1$ and $L = \omega N^2/(p_1 p_2 p_3)$; so the exponent of the measure is $\tau = 1 + \log P/\log L$, and it is below 2 exactly when $P < L$, that is, when $40 p_3^2 < \omega p_1 q_3$. This application follows Cipu, Fujita and Mignotte [10]: the proof is that of their approximation measure, with the pair coordinates (p_1, p_2, p_3) and q_3 in place of the parameters of the three-parameter family, and their constant $2.8605 \cdot 10^{28}$ becomes $2.9 \cdot 10^{28}$ because the prefactor of the bound for p_{ij} in Lemma 5.12 is taken for both signs of the representation and for the shift a_0, on the whole range $p_1 q_3 \geq 168$. We use the shifts a_0, a_1, a_2 and Rickert's approximants $p_{ij} = p_{ij}^{(k)}$ of Convention 5.1 at $x = 1/N$, whose approximated numbers are $(\vartheta_0, \vartheta_1, \vartheta_2) = (\theta_1, 1, \theta_2)$ (Lemma 5.12), $\Delta = p_1 p_2 p_3$ and $\mu = p_2/N = 2/(p_1 q_3) \leq 1/84$; in particular $N \geq 84 p_2 \geq 3 p_2$, so Lemma 5.12 applies.

We first produce the integer matrices. By Lemma 5.11, for every $k \geq 1$ the numbers $\hat{p}_{ij} = \frac{(8\Delta N)^k}{2G_k} p_{ij}(1/N)$ are integers, where G_k is the greatest common divisor of the coefficient products of order k (Convention 5.1). By Lemma 5.5, item 3, and Lemma 5.6, $G_k \geq \mathcal{P}(k) > 1.6^k/(4.09 \cdot 10^{13})$, where $\mathcal{P}(k)$ is the prime product of Definition 5.4; hence

$$\frac{(8\Delta N)^k}{2G_k} \leq \frac{4.09 \cdot 10^{13}}{2} \Bigl(\frac{8\Delta N}{1.6}\Bigr)^k = 2.045 \cdot 10^{13}\, (5\Delta N)^k.$$

The matrix $(p_{ij}(1/N))_{i,j}$ is nonsingular by Lemma 5.3, since $1/N \neq 0$; hence $\det(\hat{p}_{ij}) = \bigl((8\Delta N)^k/(2G_k)\bigr)^3 \det(p_{ij}(1/N)) \neq 0$.

We next verify the two bounds of Lemma 5.7 for the integers $p_{ijk} = \hat{p}_{ij}$. By Lemma 5.12, item 2,

$$|\hat{p}_{ij}| \leq 2.045 \cdot 10^{13} \Bigl(\frac{1 + \frac{3}{2}\mu}{1 - \mu}\Bigr)^{1/2} \Bigl(5\Delta N \cdot \frac{4}{p_1^2 p_2}\Bigr)^k = p_*\, P^k, \qquad P = \frac{20 p_3 N}{p_1},$$

with $p_* = 2.045 \cdot 10^{13}\big((1+\frac{3}{2}\mu)/(1-\mu)\big)^{1/2} \le 2.045 \cdot 10^{13} \cdot (85.5/83)^{1/2} < 2.0756 \cdot 10^{13}$. By Lemma 5.12, item 1,

$$\Big|\sum_j \hat{p}_{ij}\vartheta_j\Big| \le 2.045 \cdot 10^{13} \cdot \frac{27}{64}(1-\mu)^{-1}\Big(\frac{5\Delta N \cdot 4}{27(1-\mu)^2 N^3}\Big)^k = \ell_* L_0^{-k}, \qquad L_0 = \frac{1.35\,(1-\mu)^2 N^2}{\Delta},$$

with $\ell_* = 2.045 \cdot 10^{13} \cdot \frac{27}{64} \cdot (1-\mu)^{-1} \le 2.045 \cdot 10^{13} \cdot \frac{27}{64} \cdot \frac{84}{83} < 8.7313 \cdot 10^{12}$. The hypotheses of Lemma 5.7 hold a fortiori with p_*, ℓ_* replaced by the upper bounds $2.0756 \cdot 10^{13}$ and $8.7313 \cdot 10^{12}$, which we use from now on. Since $1.35(1-\frac{1}{84})^2 > 1.31804 > \omega$, we have $L_0 \ge L = \omega N^2/\Delta$, so the bound holds with L in place of L_0. In pair coordinates $N^2/\Delta = p_1 p_2 q_3^2/(4p_3)$ and $p_3 N/p_1 = p_2 p_3 q_3/2$, which gives the second expression of τ. Moreover $L = \omega p_1 p_2 q_3^2/(4p_3) \ge \omega \cdot 168 \cdot q_3 \cdot \frac{p_2}{4p_3} \ge 21\omega q_3 > 1$, using $p_1 q_3 \ge 168$ and $p_2 \ge p_3/2$ (as $p_1 \le p_2$ by Lemma 5.10, item 4); and $P > 1$. Hence $\tau = 1 + \log P/\log L > 1$, and the decisive comparison is that of P with L: $\tau < 2$ if and only if $P < L$, that is $20p_3 N/p_1 < \omega N^2/(p_1 p_2 p_3)$, that is $20 p_2 p_3^2 < \omega N = \frac{1}{2}\omega p_1 p_2 q_3$, that is $40 p_3^2 < \omega p_1 q_3$.

We finally apply Lemma 5.7, with the columns indexed by the shifts as explained there: for all integers A_0, A_1, A_2 with $A_0 > 0$, $\max_i |\theta_i - A_i/A_0| > C A_0^{-\tau}$ with $C^{-1} = 4p_* P(\max\{1, 2\ell_*\})^{\tau-1} = 4p_* P(2\ell_*)^{\tau-1}$. If $\tau < 2$, then $1 < \tau < 2$ gives $(2\ell_*)^{\tau-1} < 2\ell_*$ and

$$C^{-1} < 8\, p_*\, \ell_*\, P \le 8 \cdot 2.0756 \cdot 10^{13} \cdot 8.7313 \cdot 10^{12} \cdot 20\,\frac{p_3}{p_1} N < 2.9 \cdot 10^{28}\,\frac{p_3}{p_1} N.$$

The numerical constants of this proof are certified in interval arithmetic with 256-bit precision. □

5.3 The index in pair coordinates

We return to an irregular extension d with index system (λ, l, m, n). The next two lemmas, both after Cipu, Fujita and Mignotte [10], are the inputs of the index inequality Lemma 5.18: the approximation of the rescaled roots by the common term z (Lemma 5.15), and the growth of z with m (Lemma 5.16). Lemma 5.17 adds a lower bound for m that is special to pair coordinates; it is used in the first case of Theorem 5.19.

Lemma 5.15. *Let (p_1, q_1, p_2, q_2) be a pair representation of an Euler triple $\{a, b, c\}$, with rescaled roots θ_1, θ_2 (Definition 5.9). Let x, y, z be positive integers with*

$$az^2 - cx^2 = a - c, \qquad bz^2 - cy^2 = b - c.$$

Then

$$\max\Big\{\Big|\theta_1 - \frac{p_3 x}{p_1 z}\Big|, \Big|\theta_2 - \frac{p_3 y}{p_2 z}\Big|\Big\} < \frac{p_3\sqrt{c}}{2p_1\sqrt{a}}\, z^{-2}.$$

Proof. This is a lemma of Cipu, Fujita and Mignotte [10] in pair coordinates, and the proof is that of the source. By Definition 5.9, $\theta_1 = \frac{p_3}{p_1}\sqrt{a/c}$ and $\theta_2 = \frac{p_3}{p_2}\sqrt{b/c}$. Since $cx^2 - az^2 = c - a > 0$, we have $x\sqrt{c} > z\sqrt{a}$, hence

$$\Big|\theta_1 - \frac{p_3 x}{p_1 z}\Big| = \frac{p_3}{p_1 z\sqrt{c}}\,\big|z\sqrt{a} - x\sqrt{c}\big| = \frac{p_3}{p_1 z\sqrt{c}} \cdot \frac{c-a}{z\sqrt{a} + x\sqrt{c}} < \frac{p_3}{p_1 z\sqrt{c}} \cdot \frac{c}{2z\sqrt{a}} = \frac{p_3\sqrt{c}}{2p_1\sqrt{a}}\, z^{-2}.$$

In the same way, $y\sqrt{c} > z\sqrt{b}$ and

$$\Big|\theta_2 - \frac{p_3 y}{p_2 z}\Big| = \frac{p_3}{p_2 z\sqrt{c}} \cdot \frac{c-b}{z\sqrt{b} + y\sqrt{c}} < \frac{p_3\sqrt{c}}{2p_2\sqrt{b}}\, z^{-2} \le \frac{p_3\sqrt{c}}{2p_1\sqrt{a}}\, z^{-2},$$

because $p_2 \ge p_1$ (Lemma 5.10, item 4) and $b > a$. □

Lemma 5.16. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$. Then*

$$2z > \beta^{2m} > (4ac)^m.$$

Proof. The argument is that of Cipu, Fujita and Mignotte [10], without the factor 0.9999 and without a lower bound on c. Here z is the positive integer with $cd + 1 = z^2$ and $\beta = s + \sqrt{ac}$ (Definition 2.5, Definition 2.3).

We first bound z from below. By Lemma 2.15, multiplied by $\sqrt{a}$, and since $\lambda \geq -1$,

$$2z\sqrt{a} = (\sqrt{c} + \lambda\sqrt{a})\,\beta^{2m} + (\lambda\sqrt{a} - \sqrt{c})\,\beta^{-2m} \;\geq\; (\sqrt{c} - \sqrt{a})\,\beta^{2m} - (\sqrt{c} + \sqrt{a})\,\beta^{-2m}.$$

We next show that $(\sqrt{c} - 2\sqrt{a})\,\beta^{4m} > \sqrt{c} + \sqrt{a}$. By Lemma 2.4, item 4, $b \geq a + 2$ and $r \geq a + 1$, so $c - 4a = b + 2r - 3a \geq 4$, and $c > 4a$ gives $2\sqrt{a} < \sqrt{c}$; hence

$$\sqrt{c} - 2\sqrt{a} = \frac{c - 4a}{\sqrt{c} + 2\sqrt{a}} > \frac{4}{2\sqrt{c}} = \frac{2}{\sqrt{c}}.$$

Since $s^2 = ac + 1$, $s > \sqrt{ac}$ and $\beta > 2\sqrt{ac}$; as $m \geq 1$ (Lemma 2.14), $\beta^{4m} \geq \beta^4 > 16a^2c^2 \geq 16c^2$. Therefore $(\sqrt{c} - 2\sqrt{a})\beta^{4m} > 32c^{3/2} > 2\sqrt{c} > \sqrt{c} + \sqrt{a}$.

Combining, $(\sqrt{c}+\sqrt{a})\beta^{-2m} < (\sqrt{c}-2\sqrt{a})\beta^{2m}$, so $2z\sqrt{a} > (\sqrt{c}-\sqrt{a})\beta^{2m} - (\sqrt{c}-2\sqrt{a})\beta^{2m} = \sqrt{a}\,\beta^{2m}$, that is $2z > \beta^{2m}$. Finally $\beta^{2m} > (2\sqrt{ac})^{2m} = (4ac)^m$. □

Lemma 5.17. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$, and let (p_1, q_1, p_2, q_2) be a pair representation of $\{a, b, c\}$ (Definition 5.8). Then the integer*

$$\mathcal{Q} = 2(p_1m^2 + p_2n^2) + \lambda p_3(m + n)$$

is divisible by q_3 and satisfies $0 < \mathcal{Q} < 2p_3m(m + 1)$; in particular $q_3 < 2p_3m(m + 1)$.

Proof. The divisibility is the integrality of the order-two quotient $k_c = (aH + rB_n)/c$ of Convention 3.1 written in pair coordinates; here $H = H_1 + H_2$ and $B_n = 2n^2 + \lambda(m + n)$ are index polynomials, and k_c is an integer by item 2 of Lemma 3.2. Let σ be the sign of the pair representation.

We first prove that $q_3 \mid \mathcal{Q}$. By Lemma 5.10, items 1 and 2, $a = p_1q_1$, $c = p_3q_3$, $p_1q_2 = r + \sigma$, $p_3q_1 = p_1q_3 - 2\sigma$ and $p_3q_2 = p_2q_3 + 2\sigma$. Consequently

$$p_3r = p_3(p_1q_2 - \sigma) = p_1(p_2q_3 + 2\sigma) - \sigma p_3 = p_1p_2q_3 + \sigma(p_1 - p_2),$$

and

$$\begin{aligned} p_3^2q_3k_c = p_3(aH + rB_n) &= p_1(p_1q_3 - 2\sigma)H + \big(p_1p_2q_3 + \sigma(p_1 - p_2)\big)B_n \\ &= q_3p_1(p_1H + p_2B_n) - \sigma\big(2p_1H - (p_1 - p_2)B_n\big). \end{aligned}$$

Since $2H - B_n = 2m^2 + 2\lambda m + 2n^2 + 2\lambda n - 2n^2 - \lambda(m + n) = 2m^2 + \lambda(m + n)$, we have

$$2p_1H - (p_1 - p_2)B_n = p_1\big(2m^2 + \lambda(m + n)\big) + p_2\big(2n^2 + \lambda(m + n)\big) = \mathcal{Q}.$$

Hence $\sigma\mathcal{Q} = q_3\big(p_1(p_1H + p_2B_n) - p_3^2k_c\big)$, and as $\sigma = \pm 1$ and all quantities in the bracket are integers, $q_3 \mid \mathcal{Q}$.

We next prove the two bounds. By Lemma 2.14, $3 \leq n < m < l < 2n$. Write $\mathcal{Q} = p_1\big(2m^2 + \lambda(m + n)\big) + p_2\big(2n^2 + \lambda(m + n)\big)$. Both brackets are positive: for $\lambda = 1$ trivially, and for $\lambda = -1$ because $m + n < 2m \leq 2m^2$ and $m + n < 3n < 2n^2$ (as $m < 2n$ and $n \geq 3$). So $\mathcal{Q} > 0$. Since $n < m$ and $\lambda \leq 1$, $\mathcal{Q} \leq 2p_1m^2 + 2p_2n^2 + p_3(m+n) < 2p_3m^2 + 2p_3m = 2p_3m(m+1)$. Finally $\mathcal{Q}$ is a positive multiple of q_3, so $q_3 \leq \mathcal{Q} < 2p_3m(m + 1)$. □

Lemma 5.18. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$, and let (p_1, q_1, p_2, q_2) be a pair representation of $\{a, b, c\}$ with $p_1 q_3 \geq 168$ and $40\, p_3^2 < \omega\, p_1 q_3$, with ω as in Convention 5.13. Then*

$$m \log(4ac) < \log 2 + \frac{\log\bigl(\omega p_1 p_2 q_3^2/(4p_3)\bigr)}{\log\bigl(\omega p_1 q_3/(40 p_3^2)\bigr)} \cdot \log\bigl(7.3 \cdot 10^{27}\, p_2^3 p_3^3 q_3\bigr).$$

Proof. The common term z gives a simultaneous rational approximation of quality z^{-2} to the rescaled roots (θ_1, θ_2) (Lemma 5.15), while the measure of Theorem 5.14 has exponent $\tau < 2$; this bounds $\log z$ from above, and since z grows exponentially in m (Lemma 5.16), it bounds m.

Let N be the hypergeometric parameter and θ_1, θ_2 the rescaled roots of the pair representation (Definition 5.9), and let σ be its sign. Let τ be as in Theorem 5.14; by that theorem and the hypothesis $40 p_3^2 < \omega p_1 q_3$, $\tau < 2$. Explicitly, in pair coordinates

$$\tau = 1 + \frac{\log(10 p_2 p_3 q_3)}{\log\bigl(\omega p_1 p_2 q_3^2/(4p_3)\bigr)}, \qquad 2 - \tau = \frac{\log\bigl(\omega p_1 q_3/(40 p_3^2)\bigr)}{\log\bigl(\omega p_1 p_2 q_3^2/(4p_3)\bigr)} > 0,$$

as $10 p_2 p_3 q_3 > 1$ and $\omega p_1 q_3/(40 p_3^2) > 1$.

We first bound z from above. Let x, y, z be the positive integers with $ad{+}1 = x^2$, $bd{+}1 = y^2$, $cd + 1 = z^2$ (Definition 2.5); then $az^2 - cx^2 = a(cd+1) - c(ad+1) = a - c$ and likewise $bz^2 - cy^2 = b - c$. Apply Theorem 5.14 with $(A_1, A_2, A_0) = (p_2 p_3 x,\, p_1 p_3 y,\, p_1 p_2 z)$, so that $A_1/A_0 = p_3 x/(p_1 z)$ and $A_2/A_0 = p_3 y/(p_2 z)$, and compare with Lemma 5.15:

$$\Bigl(2.9 \cdot 10^{28} \frac{p_3}{p_1} N\Bigr)^{-1} (p_1 p_2 z)^{-\tau} < \max_i \Bigl|\theta_i - \frac{A_i}{A_0}\Bigr| < \frac{p_3 \sqrt{c}}{2 p_1 \sqrt{a}}\, z^{-2}.$$

Since $\tau < 2$ and $p_1 p_2 \geq 1$, $(p_1 p_2)^\tau \leq (p_1 p_2)^2$, and with $N = \frac{1}{2} p_1 p_2 q_3$,

$$z^{2-\tau} < 2.9 \cdot 10^{28}\, \frac{p_3}{p_1} \cdot \frac{p_1 p_2 q_3}{2} \cdot p_1^2 p_2^2 \cdot \frac{p_3 \sqrt{c}}{2 p_1 \sqrt{a}} = \frac{2.9 \cdot 10^{28}}{4}\, p_1 p_2^3 p_3^2 q_3 \sqrt{\frac{c}{a}}.$$

By Lemma 5.10, item 3, $\sqrt{c/a} = \frac{p_3}{p_1}\bigl(\frac{p_1 q_3}{p_1 q_3 - 2\sigma}\bigr)^{1/2} \leq \frac{p_3}{p_1}\bigl(\frac{168}{166}\bigr)^{1/2}$, as $p_1 q_3 \geq 168$ and $u \mapsto u/(u-2)$ decreases (for $\sigma = -1$ the factor $u/(u+2)$ is below 1). Hence

$$z^{2-\tau} < \frac{2.9 \cdot 10^{28}}{4} \Bigl(\frac{168}{166}\Bigr)^{1/2} p_2^3 p_3^3 q_3 < 7.3 \cdot 10^{27}\, p_2^3 p_3^3 q_3 =: \Xi.$$

Taking logarithms ($\Xi > 1$, $2 - \tau > 0$),

$$\log z < \frac{\log \Xi}{2 - \tau} = \frac{\log\bigl(\omega p_1 p_2 q_3^2/(4p_3)\bigr)}{\log\bigl(\omega p_1 q_3/(40 p_3^2)\bigr)}\, \log \Xi.$$

We next bound z from below. By Lemma 5.16, $(4ac)^m < 2z$, so $m \log(4ac) < \log z + \log 2$. Combining the two bounds gives the claim.

□

Theorem 5.19. *Let $\{a, b, c\}$ be an Euler triple with a pair representation such that*

$$p_1 q_3 \geq 800\, p_3^2, \qquad \text{or such that} \qquad p_1 q_3 \geq 42\, p_3^2 \ \text{ and } \ c \geq 4.5 \cdot 10^{12}.$$

Then $\{a, b, c\}$ has no irregular extension.

Proof. In each case the upper bound for the index m given by Lemma 5.18 contradicts the lower bounds for m given by Lemma 5.17 and Theorem 3.6 (first case) or by Theorem 3.6 alone (second case).

Suppose that $\{a,b,c\}$ has an irregular extension d, let (λ,l,m,n) be its index system (Proposition 2.11), let σ be the sign of the pair representation, and let ω be as in Convention 5.13. We first collect what both cases use. By Lemma 5.10, item 4, $1 \le p_1 \le \frac{1}{2}p_3$, so $p_3 \ge 2$. In both cases $p_1q_3 \ge 42\,p_3^2$, hence $p_1q_3 \ge 42\cdot 4 = 168$ and $40p_3^2 < 42\,\omega p_3^2 \le \omega p_1 q_3$ (as $42\omega > 40$); so Lemma 5.18 applies and gives

$$m\log(4ac) < \mathcal{R} := \log 2 + \frac{\log\bigl(\omega p_1 p_2 q_3^2/(4p_3)\bigr)}{\log\bigl(\omega p_1 q_3/(40p_3^2)\bigr)} \cdot \log\bigl(7.3\cdot 10^{27}\, p_2^3 p_3^3 q_3\bigr).$$

The three logarithms in $\mathcal{R}$ are positive: $\omega p_1q_3/(40p_3^2) > 1$ as just shown, $7.3\cdot 10^{27}p_2^3p_3^3q_3 > 1$, and $\omega p_1p_2q_3^2/(4p_3) = 10p_2p_3q_3\cdot \omega p_1q_3/(40p_3^2) > 1$. Hence $\mathcal{R}$ can only increase when the two logarithms of the numerator are replaced by upper bounds and the logarithm of the denominator by a positive lower bound. On the other side, by Theorem 3.6, $c < 8m^4$, that is

$$2m > (2c)^{1/4},$$

and by Lemma 5.17, $q_3 < 2p_3m(m+1)$, that is

$$m(m+1) > \frac{q_3}{2p_3}.$$

We now treat the case $p_1q_3 \ge 800\,p_3^2$. Put $u := q_3/(2p_3)$. Since $p_1 \le \frac{1}{2}p_3$, $u \ge p_1q_3/p_3^2 \ge 800$, and $c = p_3q_3 = 2up_3^2$ (Lemma 5.10, item 2). Moreover $p_3q_1 = p_1q_3 - 2\sigma \ge 800\,p_3^2 - 2$ (Lemma 5.10, item 2), so

$$a = p_1q_1 \ge q_1 \ge 800\,p_3 - \frac{2}{p_3} \ge 799.5\,p_3, \qquad 4ac \ge 8\cdot 799.5\,up_3^3 = 6396\,up_3^3.$$

The two lower bounds for m read

$$m > \sqrt{u+\frac{1}{4}} - \frac{1}{2} \qquad \text{and} \qquad m > \frac{1}{2}(2c)^{1/4} = \Bigl(\frac{up_3^2}{4}\Bigr)^{1/4}.$$

On the other hand, $p_1p_2 \le \frac{1}{4}p_3^2$, $p_2 < p_3$, $q_3 = 2up_3$ and $\log\bigl(\omega p_1q_3/(40p_3^2)\bigr) \ge \log(800\,\omega/40) = \log(20\omega) > 0$, so the bound $m\log(4ac) < \mathcal{R}$ yields

$$m\log(6396\,up_3^3) \le m\log(4ac) < \log 2 + \frac{\log(\omega u^2 p_3^3/4)}{\log(20\omega)}\log\bigl(1.46\cdot 10^{28}\,up_3^7\bigr) =: R^*(u,p_3).$$

We next show that the contradiction need only be checked at $u = 800$. Fix $p_3 \ge 2$, put $\xi = \log u$, $\eta = \log p_3$ and $w_0 = 1/\log(20\omega) < 0.306$, and consider

$$g_1(u) = \Bigl(\sqrt{u+\tfrac{1}{4}} - \tfrac{1}{2}\Bigr)\log(6396\,up_3^3) - R^*(u,p_3),$$
$$g_2(u) = \Bigl(\frac{up_3^2}{4}\Bigr)^{1/4}\log(6396\,up_3^3) - R^*(u,p_3).$$

Here $R^*(u,p_3) = \log 2 + w_0\bigl(2\xi+3\eta+\log(\omega/4)\bigr)\bigl(\xi+7\eta+\log(1.46\cdot 10^{28})\bigr)$, so

$$u\,\partial_u R^*(u,p_3) = w_0\bigl(4\xi+17\eta+2\log(1.46\cdot 10^{28})+\log(\omega/4)\bigr) < 1.23\xi + 5.21\eta + 39.4.$$

On the other hand, $\log(6396\,up_3^3) = \xi + 3\eta + \log 6396 > \xi + 3\eta + 8.76$. For $u \ge 800$ we have $u/(2\sqrt{u+1/4}) > 14.1$, so

$$u\,\partial_u\Big[\Big(\sqrt{u+\tfrac14}-\tfrac12\Big)\log(6396\,up_3^3)\Big] > 14.1(\xi+3\eta+8.76) > 1.23\xi + 5.21\eta + 39.4.$$

For $u \ge 800$ and $p_3 \ge 55$ we have $(up_3^2/4)^{1/4} > 27.8$, so

$$\begin{aligned} u\,\partial_u\Big[\Big(\frac{up_3^2}{4}\Big)^{1/4}\log(6396\,up_3^3)\Big] &= \Big(\frac{up_3^2}{4}\Big)^{1/4}\Big(\frac{\xi+3\eta+\log 6396}{4}+1\Big) \\ &> 27.8\Big(\frac{\xi+3\eta+8.76}{4}+1\Big) > 1.23\xi + 5.21\eta + 39.4. \end{aligned}$$

Hence g_1 is strictly increasing on $[800,\infty)$ for every $p_3 \ge 2$, and g_2 is strictly increasing on $[800,\infty)$ for every $p_3 \ge 55$. The contradiction to be derived is $g_1(u) > 0$ for $2 \le p_3 \le 55$ and $g_2(u) > 0$ for $p_3 \ge 55$, so it suffices to establish it at $u = 800$.

We now treat $u = 800$ and $2 \le p_3 \le 55$, with $\eta = \log p_3 \ge \log 2$. Using $m > \sqrt{800.25} - 0.5$, the difference

$$\begin{aligned} f_1(\eta) := (\sqrt{800.25}-0.5)\big(\log(5\,116\,800)+3\eta\big) - \log 2 \\ - \frac{(\log(160\,000\,\omega)+3\eta)(\log(1.168\cdot 10^{31})+7\eta)}{\log(20\omega)} \end{aligned}$$

is a strictly concave quadratic polynomial in η, since its second derivative is $-42/\log(20\omega) < 0$. Interval evaluation at the endpoints, in 256-bit arithmetic, gives $f_1(\log 2) > 151.5836$ and $f_1(\log 55) > 23.5355$, so by concavity $f_1(\log p_3) > 0$ for all $p_3 \in [2,55]$.

We next treat $u = 800$ and $p_3 \ge 55$. Using $m > (200\,p_3^2)^{1/4} = 200^{1/4}e^{\eta/2}$, the function

$$f_2(\eta) := 200^{1/4}e^{\eta/2}\big(\log(5\,116\,800)+3\eta\big) - R^*(800, e^{\eta})$$

satisfies $f_2(\log 55) > 26.3014$, by the same interval evaluation. Its derivative is positive for $\eta \ge \eta_0 := \log 55$. Indeed, with $w_1 = \log(5\,116\,800)$, $\xi_0 = \log 800$, $C_1 = 2\xi_0 + \log(\omega/4)$ and $C_2 = \xi_0 + \log(1.46\cdot 10^{28})$,

$$f_2'(\eta) = 200^{1/4}e^{\eta/2}\Big(\frac{w_1+3\eta}{2}+3\Big) - w_0\big(42\eta + 3C_2 + 7C_1\big).$$

By convexity $e^{\eta/2} \ge e^{\eta_0/2}\big(1+\frac{v}{2}\big)$ with $v = \eta - \eta_0 \ge 0$, so the first term is at least $200^{1/4}\sqrt{55}\,\big(1+\frac{v}{2}\big)\big(\frac{w_1+3\eta_0}{2}+3+\frac{3}{2}v\big) > 466 + 275v$, while the second is less than $145 + 13v$.

Thus $f_2(\log p_3) > 0$ for all $p_3 \ge 55$. In both ranges the two lower bounds for m contradict the upper bound $m\log(4ac) < \mathcal{R}$, which settles the first case.

We finally treat the case $p_1q_3 \ge 42\,p_3^2$ and $c \ge 4.5\cdot 10^{12}$, by an argument of Cipu, Fujita and Mignotte [10] in pair coordinates, with their congruence lower bound for m replaced by the quartic index floor of Theorem 3.6. We first bound $\mathcal{R}$ by a function of c alone. By Lemma 5.10, item 2, $c = p_3q_3$; moreover $p_1p_2 \le \frac14 p_3^2$ by the AM–GM inequality, and $p_3 \ge 2$. Hence

$$\frac{\omega p_1p_2q_3^2}{4p_3} \le \frac{\omega p_3q_3^2}{16} = \frac{\omega c^2}{16p_3} \le \frac{\omega c^2}{32}; \qquad \frac{\omega p_1q_3}{40p_3^2} \ge \frac{42\,\omega}{40} > 1.$$

Moreover $p_1 \le \frac12 p_3$ gives $42p_3^2 \le p_1q_3 \le \frac12 p_3q_3 = \frac12 c$, so $p_3 \le (c/84)^{1/2}$, and with $p_2 < p_3$, $q_3 = c/p_3$,

$$7.3\cdot 10^{27}p_2^3p_3^3q_3 < 7.3\cdot 10^{27}p_3^5\,c \le \frac{7.3\cdot 10^{27}}{84^{5/2}}\,c^{7/2}.$$

On the left, $2m > (2c)^{1/4}$, and $\log(4ac) \geq \log(4c)$ as $a \geq 1$. Put $\zeta = \log c$, $A = 7.3 \cdot 10^{27}/84^{5/2}$ and, for real ζ,

$$\phi(\zeta) = \frac{2^{1/4}}{2}\, e^{\zeta/4}(\zeta + \log 4) - \log 2 - \frac{\big(2\zeta + \log \frac{\omega}{32}\big)\big(\frac{7}{2}\zeta + \log A\big)}{\log \frac{42\omega}{40}}.$$

Since $\frac{1}{2}(2c)^{1/4}\log(4c) = \frac{2^{1/4}}{2}e^{\zeta/4}(\zeta+\log 4)$, $\log(\omega c^2/32) = 2\zeta+\log\frac{\omega}{32}$ and $\log(Ac^{7/2}) = \frac{7}{2}\zeta+\log A$, these bounds turn $m\log(4ac) < \mathcal{R}$ into $\phi(\log c) < 0$.

We now show that $\phi \geq 0$ on $[\zeta_1, \infty)$, where $\zeta_1 = \log(4.5 \cdot 10^{12})$; since $\log c \geq \zeta_1$, this contradicts $\phi(\log c) < 0$. Differentiating twice,

$$\phi''(\zeta) = \frac{2^{1/4}}{2}\, e^{\zeta/4}\Big(\frac{\zeta + \log 4}{16} + \frac{1}{2}\Big) - \frac{14}{\log \frac{42\omega}{40}},$$

and the first term has derivative $\frac{2^{1/4}}{2}e^{\zeta/4}\big(\frac{\zeta+\log 4}{64} + \frac{3}{16}\big) > 0$ for $\zeta > -12 - \log 4$. As $\zeta_1 > 29 > -12-\log 4$, ϕ'' is increasing on $[\zeta_1, \infty)$. Hence, if $\phi''(\zeta_1) \geq 0$, then ϕ' is non-decreasing on $[\zeta_1, \infty)$; and if moreover $\phi(\zeta_1) \geq 0$ and $\phi'(\zeta_1) \geq 0$, then for $\zeta \geq \zeta_1$, $\phi(\zeta) = \phi(\zeta_1) + \int_{\zeta_1}^{\zeta} \phi' \geq \phi(\zeta_1) + (\zeta - \zeta_1)\phi'(\zeta_1) \geq 0$. In interval arithmetic with 256-bit precision, $\phi(\zeta_1) > 115.1$, $\phi'(\zeta_1) > 5924$ and $\phi''(\zeta_1) > 2041$. Hence $\phi(\log c) \geq 0$, a contradiction, which settles the second case. So $\{a, b, c\}$ has no irregular extension.

□

Since $p_1q_3 = p_3q_1 + 2\sigma$ (Lemma 5.10, item 2), the hypotheses $p_1q_3 \geq 800\,p_3^2$ and $p_1q_3 \geq 42\,p_3^2$ say, up to the term 2σ, that $q_1 \geq 800\,p_3$ and $q_1 \geq 42\,p_3$: the smallest element $a = p_1q_1$ has a factor q_1 that is large compared with $p_1 + p_2$. This is the case in the three-parameter family of Section 8, for which item 3 of Lemma 8.2 gives $p_1q_3 \geq \frac{K-2}{3}\,p_3^2$. The criterion is applied there, and Lemma 5.18 once more in Appendix A.

6 Coprime divisors of the index combinations

This section proves Theorem 6.3, a lower bound for the index of another kind than the quartic floor. The quartic floor (Theorem 3.6) bounds m from below by a power of c. Theorem 6.3 shows that three coprime divisors of the triple, built from greatest common divisors of two elements or of an element and a root, divide the index combinations $m - n$, $l + \lambda m$ and $l + \lambda n$; through the gap inequality $n > (m-n)R_z$ (Lemma 2.18, item 3) the first of them bounds m from below. Its one application, to the triples with two elements in a fixed ratio, is in Subsection 8.2. The whole argument lies in the proof of the theorem, which works with the matrix form of an index system (Lemma 2.8, item 2); the lemma before it is a two-line coprimality check.

Definition 6.1. Let $\{a, b, c\}$ be an Euler triple with roots r, s, t (Definition 2.3). Its **gcd divisors** are

$$\Delta_{ab} = \frac{\gcd(a,b)}{\gcd(a,b,4)}, \qquad \Delta_{bc} = \frac{\gcd(b,c)}{\gcd(b,c,4)}, \qquad \Delta_{ac} = \frac{\gcd(a,c)}{\gcd(a,c,4)},$$

its **root divisors** are

$$G_{rc} = \frac{\gcd(r,c)}{\gcd(r,c,2)}, \qquad G_{ta} = \frac{\gcd(t,a)}{\gcd(t,a,2)}, \qquad G_{sb} = \frac{\gcd(s,b)}{\gcd(s,b,2)},$$

and its **coprime divisors** are the products

$$\Pi_1 = \Delta_{ab} G_{rc}, \qquad \Pi_2 = \Delta_{bc} G_{ta}, \qquad \Pi_3 = \Delta_{ac} G_{sb}.$$

The three **index combinations** of an index system (λ, l, m, n) of an extension of $\{a, b, c\}$ (Definition 2.5) are numbered

$$1: \ m - n, \qquad 2: \ l + \lambda m, \qquad 3: \ l + \lambda n,$$

and objects attached to them carry the same number and are listed in this order. The pair of elements and the element–root pair attached to them are $\{a, b\}$ and $\{r, c\}$ for 1, $\{b, c\}$ and $\{t, a\}$ for 2, $\{a, c\}$ and $\{s, b\}$ for 3.

Each index combination receives two divisors, one from a pair of elements and one from an element and a root. The factors $\gcd(\cdot, 4)$ and $\gcd(\cdot, 2)$ are removed because the congruences in the proof of Theorem 6.3 hold for 4 and 2 times the combination, respectively. The two divisors attached to one combination are coprime by the next lemma, so that with each of them their product Π_i divides the combination.

Lemma 6.2. *For every Euler triple $\{a, b, c\}$, the gcd divisors and the root divisors (Definition 6.1) satisfy*

$$\gcd(\Delta_{ab}, G_{rc}) = \gcd(\Delta_{bc}, G_{ta}) = \gcd(\Delta_{ac}, G_{sb}) = 1.$$

Proof. By Definition 6.1, $\Delta_{ab} \mid a$ and $G_{rc} \mid r$, $\Delta_{bc} \mid b$ and $G_{ta} \mid t$, $\Delta_{ac} \mid a$ and $G_{sb} \mid s$. By Lemma 2.4, item 3, $\gcd(a, r) = \gcd(b, t) = \gcd(a, s) = 1$. Hence a common divisor of Δ_{ab} and G_{rc} divides $\gcd(a, r) = 1$, a common divisor of Δ_{bc} and G_{ta} divides $\gcd(b, t) = 1$, and a common divisor of Δ_{ac} and G_{sb} divides $\gcd(a, s) = 1$. □

Theorem 6.3. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$, with the coprime divisors Π_1, Π_2, Π_3 of Definition 6.1 and the gap ratio R_z of Definition 2.16. Then*

$$\Pi_1 \mid m - n, \qquad \Pi_2 \mid l + \lambda m, \qquad \Pi_3 \mid l + \lambda n, \qquad \textit{and} \qquad m > \Pi_1 (1 + R_z).$$

Proof. We reduce the three displays of Definition 2.5 modulo each of the six integers $\gcd(a, b)$, $\gcd(b, c)$, $\gcd(a, c)$, $\gcd(r, c)$, $\gcd(t, a)$ and $\gcd(s, b)$: modulo each of them the squares of the multiplication matrices are unipotent or $-\mathbf{I}$, so the displays become linear congruences in l, m, n, which give the three divisibilities; the gap inequality then gives the lower bound for m. Congruences modulo factors of c are used in [10]; here the moduli are these six greatest common divisors. Throughout, $c = a + b + 2r$, $s = a + r$, $t = b + r$ and $r^2 = ab + 1$, and $s^2 = ac + 1$, $t^2 = bc + 1$ by Lemma 2.4, item 1. Let $\mathbf{A}, \mathbf{B}, \mathbf{C}$ be the multiplication matrices of $\{a, b, c\}$ (Definition 2.3), and let x, y, z be as in Definition 2.5.

We first write the index system in matrix form: by item 2 of Lemma 2.8,

$$\begin{pmatrix} y \\ x \end{pmatrix} = \mathbf{A}^{2l} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} z \\ x \end{pmatrix} = \mathbf{B}^{2m} \begin{pmatrix} \lambda \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} z \\ y \end{pmatrix} = \mathbf{C}^{2n} \begin{pmatrix} \lambda \\ 1 \end{pmatrix}.$$

We next record the squares of the multiplication matrices and the powers of special matrices modulo an integer. By $r^2 = ab+1$, $s^2 = ac+1$ and $t^2 = bc+1$,

$$\mathbf{A}^2 = \begin{pmatrix} 2ab+1 & 2rb \\ 2ra & 2ab+1 \end{pmatrix}, \qquad \mathbf{B}^2 = \begin{pmatrix} 2ac+1 & 2sc \\ 2sa & 2ac+1 \end{pmatrix}, \qquad \mathbf{C}^2 = \begin{pmatrix} 2bc+1 & 2tc \\ 2tb & 2bc+1 \end{pmatrix}.$$

Modulo any integer, a matrix congruent to $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, to $\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$ or to $-\mathbf{I}$ has k-th power congruent to $\begin{pmatrix} 1 & ku \\ 0 & 1 \end{pmatrix}$, to $\begin{pmatrix} 1 & 0 \\ ku & 1 \end{pmatrix}$ or to $(-1)^k\mathbf{I}$, for every $k \geq 0$. Modulo each of the six greatest common divisors above, the squares $\mathbf{A}^2, \mathbf{B}^2, \mathbf{C}^2$ are of one of these three shapes, so the three matrix equations above become linear in l, m, n; we compare a coordinate that two of them share. All congruences below are modulo the integer g named at the start of the paragraph.

Modulo $g = \gcd(a,b)$: $r^2 \equiv 1$, $c \equiv 2r$ and $s \equiv t \equiv r$, so $\mathbf{B}^2 \equiv \begin{pmatrix} 1 & 2sc \\ 0 & 1 \end{pmatrix}$ and $\mathbf{C}^2 \equiv \begin{pmatrix} 1 & 2tc \\ 0 & 1 \end{pmatrix}$. The first coordinates of the second and third equations give $z \equiv \lambda + 2msc \equiv \lambda + 2ntc$, hence $0 \equiv 2rc(m-n) \equiv 4r^2(m-n) \equiv 4(m-n)$.

Modulo $g = \gcd(b,c)$: $r^2 \equiv 1$, $a \equiv -2r$ and $s \equiv -r$, so $\mathbf{A}^2 \equiv \begin{pmatrix} 1 & 0 \\ 2ra & 1 \end{pmatrix}$ and $\mathbf{B}^2 \equiv \begin{pmatrix} 1 & 0 \\ 2sa & 1 \end{pmatrix}$. The second coordinates of the first two equations give $x \equiv 1 + 2lra \equiv 1 + 2\lambda msa$, hence $0 \equiv 2a(lr - \lambda ms) \equiv 2ar(l + \lambda m) \equiv -4r^2(l+\lambda m) \equiv -4(l+\lambda m)$.

Modulo $g = \gcd(a,c)$: $r^2 \equiv 1$, $b \equiv -2r$ and $t \equiv -r$, so $\mathbf{A}^2 \equiv \begin{pmatrix} 1 & 2rb \\ 0 & 1 \end{pmatrix}$ and $\mathbf{C}^2 \equiv \begin{pmatrix} 1 & 0 \\ 2tb & 1 \end{pmatrix}$. The coordinate y of the first and third equations gives $y \equiv 1 + 2lrb \equiv 1 + 2\lambda ntb$, hence $0 \equiv 2b(lr - \lambda nt) \equiv 2br(l+\lambda n) \equiv -4r^2(l+\lambda n) \equiv -4(l+\lambda n)$.

Modulo $g = \gcd(r,c)$: $b \equiv -a$ and $ab \equiv -1$, so $a^2 \equiv 1$, $s \equiv a$ and $t \equiv -a$. Then $\mathbf{A}^2 \equiv -\mathbf{I}$, so $x \equiv y \equiv (-1)^l$, while $\mathbf{B}^2 \equiv \mathbf{C}^2 \equiv \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, so $x \equiv 1 + 2\lambda m$ and $y \equiv 1 + 2\lambda n$. Hence $2\lambda m \equiv 2\lambda n$, that is $2(m-n) \equiv 0$, since $\lambda = \pm 1$.

Modulo $g = \gcd(t,a)$: $r \equiv -b$, $b^2 \equiv r^2 \equiv 1$, $c \equiv -b$ and $s \equiv -b$. Then $\mathbf{C}^2 \equiv -\mathbf{I}$, so $z \equiv \lambda y$; $\mathbf{A}^2 \equiv \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$ gives $y \equiv 1 - 2l$; and $\mathbf{B}^2 \equiv \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ gives $z \equiv \lambda + 2m$. Hence $\lambda + 2m \equiv \lambda - 2\lambda l$, that is $2(m + \lambda l) \equiv 0$, and multiplying by λ, $2(l + \lambda m) \equiv 0$.

Modulo $g = \gcd(s,b)$: $r \equiv -a$, $a^2 \equiv r^2 \equiv 1$, $c \equiv -a$ and $t \equiv -a$. Then $\mathbf{B}^2 \equiv -\mathbf{I}$, so $z \equiv \lambda x$; $\mathbf{A}^2 \equiv \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$ gives $x \equiv 1 - 2l$; and $\mathbf{C}^2 \equiv \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ gives $z \equiv \lambda + 2n$. Hence $\lambda + 2n \equiv \lambda - 2\lambda l$, that is $2(n + \lambda l) \equiv 0$, and multiplying by λ, $2(l + \lambda n) \equiv 0$.

We next pass to the divisors. The six congruences just proved say that

$$\gcd(a,b) \mid 4(m-n), \qquad \gcd(b,c) \mid 4(l+\lambda m), \qquad \gcd(a,c) \mid 4(l+\lambda n),$$

$$\gcd(r,c) \mid 2(m-n), \qquad \gcd(t,a) \mid 2(l+\lambda m), \qquad \gcd(s,b) \mid 2(l+\lambda n).$$

If $g \mid 4k$ for integers $g \geq 1$ and k, then $\frac{g}{\gcd(g,4)} \mid k$, and if $g \mid 2k$, then $\frac{g}{\gcd(g,2)} \mid k$.

Since $\gcd(a,b,4) = \gcd(\gcd(a,b),4)$ and $\gcd(r,c,2) = \gcd(\gcd(r,c),2)$, and likewise for the other four, it follows by Definition 6.1 that Δ_{ab} and G_{rc} divide $m-n$, Δ_{bc} and G_{ta} divide $l+\lambda m$, and Δ_{ac} and G_{sb} divide $l + \lambda n$. The two divisors in each pair are coprime by Lemma 6.2, so their products, the coprime divisors, satisfy

$$\Pi_1 \mid m-n, \qquad \Pi_2 \mid l+\lambda m, \qquad \Pi_3 \mid l+\lambda n.$$

We finally prove $m > \Pi_1(1+R_z)$. By Lemma 2.14, $3 \le n < m < l < 2n$. In particular $m-n \ge 1$, and as $\Pi_1 \mid m-n$, $m-n \ge \Pi_1$. By the gap inequality of Lemma 2.18, item 3, $n > (m-n)R_z$, where $R_z = \frac{\sqrt{ac}}{b-a}\log\beta > 0$ is the gap ratio of Definition 2.16. Hence

$$m = n + (m-n) > (m-n)(1+R_z) \ge \Pi_1(1+R_z).$$

□

7 An effective bound for irregular extensions

This section proves the effective bound (Theorem 7.9), $c < 4 \cdot 10^{48}$. Its ceilings for the index come from lower bounds for linear forms in three logarithms, applied to the form $\Lambda_x = 2l\log\alpha - 2m\log\beta + \log D_\lambda$ of Definition 2.16, which is positive and smaller than $4.01\,\beta^{-4m}$ (Lemma 2.18, item 4); the sizes and heights of α, β and D_λ are those of Lemma 4.2. These bounds enter at two levels of precision. In Subsection 7.1, Matveev's theorem [23] gives the a priori bound for the index (Proposition 7.3), valid for every irregular extension, and against the quartic index floor (Theorem 3.6) it gives $c < 10^{75}$ (Proposition 7.5). In Subsection 7.2, the theorem of Mignotte and Voutier [24] gives caps for m, from $m < 7 \cdot 10^{12}$ down to $m < 10^{12}$, on four windows of c (Proposition 7.8). This proposition is the heart of the section; its main step excludes an exceptional linear relation between the coefficients of Λ_x, with Laurent's theorem (Theorem 4.3) from Section 4. The effective bound then follows by feeding each cap back into the quartic floor.

7.1 The a priori bound

Convention 7.1. The **a priori function** is defined, for real $c > 1$ and $u \ge 1$, by

$$\Phi_c(u) = u - 0.15 - K_E(\log c)^2 \log(19.46\,u), \qquad K_E = 2.4638 \cdot 10^{12}.$$

Its constants K_E, 0.15 and 19.46 are those of the a priori bound for the index, obtained from Matveev's theorem applied to the linear form Λ_x (Definition 2.16).

The function Φ_c is the a priori bound in the form in which it is used: a single value $u_0 \ge 1$ with $\Phi_c(u_0) \ge 0$ caps the index by $2m < u_0$ (Proposition 7.3). It is used in this form in this section, in Section 8 and in Appendix B.

Theorem 7.2. *Let $\mathcal{L}$ be a real number field of degree $\mathcal{D}$, let $\eta_1, \eta_2, \eta_3 \in \mathcal{L}$ be positive and multiplicatively independent, and let $b_1, b_2, b_3 \in \mathbb{Z}$ with $b_3 \ne 0$ and*

$$\Lambda_M = b_1\log\eta_1 + b_2\log\eta_2 + b_3\log\eta_3.$$

Let A_1, A_2, A_3 be real numbers with $A_i \ge \max\{\mathcal{D}\,\mathrm{h}(\eta_i), |\log\eta_i|, 0.16\}$ (Definition 4.1), and put $B_M = \max\{1, |b_1|A_1/A_3, |b_2|A_2/A_3, |b_3|\}$. Then

$$\log|\Lambda_M| > -C_M(3)\,C_0\,W_0\,\mathcal{D}^2\,A_1A_2A_3,$$

where $C_M(3) = \frac{16}{3!}e^3 \cdot 9 \cdot 5 \cdot 16^4 \cdot \frac{3e}{2} < 6.441 \cdot 10^8$, $C_0 = \log\bigl(e^{20.2}3^{5.5}\mathcal{D}^2\log(e\mathcal{D})\bigr)$ and $W_0 = \log\bigl(1.5e\,B_M\mathcal{D}\log(e\mathcal{D})\bigr)$.

Proof. This is Matveev's theorem [23] for three logarithms in a real field; the condition $A_i \ge 0.16$ only restricts the admissible choices of A_i. With $A_j = \max\{\mathcal{D}\,\mathrm{h}(\eta_j), |\log\eta_j|\}$ it is stated in [18, Proposition 6.2], with the constant $11796480\,e^4\mathcal{D}^2\log\bigl(3^{5.5}e^{20.2}\mathcal{D}^2\log(e\mathcal{D})\bigr)$, which is $C_M(3)C_0\mathcal{D}^2$ because $11796480 = \frac{16}{6} \cdot 9 \cdot 5 \cdot 16^4 \cdot \frac{3}{2}$. □

Proposition 7.3. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$, and let Φ_c be as in Convention 7.1. Then $\Phi_c(2m) < 0$; consequently $2m < u_0$ for every real $u_0 \geq 1$ with $\Phi_c(u_0) \geq 0$.*

Proof. We apply Matveev's theorem (Theorem 7.2) to the linear form Λ_x of Definition 2.16.

We first collect the inputs. By Lemma 2.14, $m \geq 4$ and $c > b > 4000$. By Lemma 2.18, $l \log\alpha < m \log\beta$ (item 1) and $0 < \Lambda_x < 4.01\,\beta^{-4m}$ (item 4). By Lemma 4.2: $\log\alpha < \log c$ and $\frac{1}{2}\log c + \log 2 < \log\beta < \log c$ (item 1); $\mathcal{K}$ is a real biquadratic field (item 2); $\mathrm{h}(\alpha) = \frac{1}{2}\log\alpha$ and $\mathrm{h}(\beta) = \frac{1}{2}\log\beta$ (item 3); $0 < \log D_\lambda < \log 4$ and $\mathrm{h}(D_\lambda) < \log c$ (item 4); and $\alpha, \beta/\alpha, D_\lambda$ exceed 1 and are multiplicatively independent (item 6).

We next choose the parameters of Theorem 7.2. Take $\mathcal{L} = \mathcal{K}$, which contains α, β and D_λ and has degree $\mathcal{D} = 4$; take $\eta_1 = \alpha$, $\eta_2 = \beta$, $\eta_3 = D_\lambda$ and $b_1 = 2l$, $b_2 = -2m$, $b_3 = 1$, so that $\Lambda_M = \Lambda_x$. The η_i are positive, and multiplicatively independent because they generate the same group as $\alpha, \beta/\alpha, D_\lambda$; $b_3 \neq 0$. We may take

$$A_1 = 2\log\alpha, \qquad A_2 = 2\log\beta, \qquad A_3 = 4\log c,$$

since $4\,\mathrm{h}(\alpha) = 2\log\alpha$, $4\,\mathrm{h}(\beta) = 2\log\beta$, $4\,\mathrm{h}(D_\lambda) < 4\log c$, $\log D_\lambda < \log 4 < 4\log c$, and all three exceed 0.16 because $\log c > \log 4000$ and $2\log\alpha > \log c$ (item 1 of Lemma 4.2). As $l\log\alpha < m\log\beta$, $\log\beta < \log c$ and $m \geq 4$,

$$B_M = \max\Big\{1, \frac{l\log\alpha}{\log c}, \frac{m\log\beta}{\log c}\Big\} \leq m,$$

so $W_0 = \log\big(1.5e\,B_M\mathcal{D}\log(e\mathcal{D})\big) \leq \log\big(0.75e\,\mathcal{D}\log(e\mathcal{D})\cdot 2m\big) < \log(19.46\cdot 2m)$.

We now prove that $\Phi_c(2m) < 0$. Put $\widehat{C} = C_M(3)C_0\mathcal{D}^2$. Theorem 7.2 gives $\log\Lambda_x > -\widehat{C}\,W_0A_1A_2A_3 = -16\,\widehat{C}\,W_0\log\alpha\log\beta\log c$, and $\Lambda_x < 4.01\,\beta^{-4m}$ gives $\log\Lambda_x < \log 4.01 - 4m\log\beta$. Hence $4m\log\beta < \log 4.01 + 16\,\widehat{C}\,W_0\log\alpha\log\beta\log c$; dividing by $2\log\beta$ and using $\log\alpha < \log c$ and $2\log\beta > \log 4000 + 2\log 2$,

$$2m < \frac{\log 4.01}{\log 4000 + 2\log 2} + 8\widehat{C}(\log c)^2\log(19.46\cdot 2m) < 0.15 + K_E(\log c)^2\log(19.46\cdot 2m),$$

that is, $\Phi_c(2m) < 0$. The constants of Φ_c enter through three numerical bounds, $8\widehat{C} < K_E$, $\log 4.01/(\log 4000 + 2\log 2) < 0.15$ and $0.75e\,\mathcal{D}\log(e\mathcal{D}) < 19.46$, which were verified in interval arithmetic with outward rounding.

For the second assertion, let $u_0 \geq 1$ with $\Phi_c(u_0) \geq 0$. Since $\log(19.46\,u_0) > 1$, $u_0 > K_E(\log c)^2\log(19.46\,u_0) > K_E(\log c)^2$, and $\Phi_c'(u) = 1 - K_E(\log c)^2/u > 0$ for $u \geq u_0$; so Φ_c is strictly increasing on $[u_0, \infty)$. If $2m \geq u_0$, then $\Phi_c(2m) \geq \Phi_c(u_0) \geq 0$, contradicting the first assertion. Hence $2m < u_0$. □

To use the cap one needs a point at which Φ_c is positive for all large c at once. The next lemma gives such points along curves $u = \iota c^\theta$, from a check at a single value c_0. It is developed once and used twice: with $(\iota, \theta, c_0) = (2^{1/4}, \frac{1}{4}, 10^{75})$, against the quartic floor, in Proposition 7.5; and with $(\iota, \theta, c_0) = (1/1806, 1, 10^{21})$, against the floor from coprime divisors, which is linear in c, in Theorem 8.7.

Lemma 7.4. *Let Φ_c and K_E be as in Convention 7.1. Let $\iota > 0$, $\theta > 0$ and $c_0 > 1$ satisfy $\iota c_0^\theta \geq 1$, $\theta\log c_0 \geq 2 + |\log(19.46\,\iota)|$,*

$$\Phi_{c_0}(\iota c_0^\theta) > 0 \qquad \text{and} \qquad \theta\iota c_0^\theta > K_E\log c_0\,\big(2\log(19.46\,\iota c_0^\theta) + \theta\log c_0\big).$$

Then $\Phi_c(\iota c^\theta) > 0$ for every real $c \geq c_0$.

Proof. Put $\ell = \log(19.46\iota)$ and $w = \theta \log c$, so that $\iota c^\theta = \iota e^w \geq 1$ for $c \geq c_0$ and $\log(19.46\iota c^\theta) = \ell + w$. Then $\Phi_c(\iota c^\theta) = f(w)$, where

$$f(w) = \iota e^w - P(w), \qquad P(w) = 0.15 + \frac{K_E}{\theta^2}\, w^2(\ell + w).$$

Put $w_0 = \theta \log c_0$. It suffices to show that $f(w) > 0$ for $w \geq w_0$. We have

$$P'(w) = \frac{K_E}{\theta^2}\,(3w^2 + 2\ell w), \qquad P''(w) = \frac{K_E}{\theta^2}\,(6w + 2\ell),$$
$$\frac{\theta^2}{K_E}\big(P'(w) - P''(w)\big) = 3w(w-2) + 2\ell(w-1).$$

For $w \geq w_0 \geq 2 + |\ell|$ the last quantity is nonnegative: if $\ell \geq 0$ both terms are nonnegative, and if $\ell < 0$ then $3w(w-2) \geq 3w|\ell| \geq 2|\ell|(w-1)$. Hence $P'' \leq P'$ on $[w_0, \infty)$.

Let $g = f' = \iota e^w - P'$. On $[w_0, \infty)$ we have $g' = \iota e^w - P'' \geq g$, so $(e^{-w} g)' \geq 0$ and $g(w) \geq g(w_0)\, e^{w - w_0}$. Moreover

$$\theta\, g(w_0) = \theta \iota c_0^\theta - K_E \log c_0\,(3w_0 + 2\ell) = \theta \iota c_0^\theta - K_E \log c_0\,\big(2\log(19.46\,\iota c_0^\theta) + \theta \log c_0\big) > 0$$

by hypothesis. Hence $g > 0$ on $[w_0, \infty)$, so f is increasing there, and $f(w) \geq f(w_0) = \Phi_{c_0}(\iota c_0^\theta) > 0$ for $w \geq w_0$. □

Proposition 7.5. *Let d be an irregular extension of an Euler triple $\{a, b, c\}$. Then $c < 10^{75}$.*

Proof. We compare the quartic index floor with the a priori bound along the curve $u = 2^{1/4} c^{1/4}$. Let (λ, l, m, n) be the index system of d (Proposition 2.11), let Φ_c and K_E be as in Convention 7.1, and suppose that $c \geq 10^{75}$.

By Theorem 3.6, $c < 8m^4$, hence

$$2m > 2\Big(\frac{c}{8}\Big)^{1/4} = \iota\, c^{1/4}, \qquad \iota = 2^{1/4}.$$

We apply Lemma 7.4 with $\iota = 2^{1/4}$, $\theta = \frac{1}{4}$ and $c_0 = 10^{75}$, and check its four hypotheses. First, $\iota c_0^\theta = 2^{1/4} 10^{75/4} > 6.68 \cdot 10^{18} \geq 1$. Second, $\theta \log c_0 = \frac{75}{4} \log 10 > 43.17$, while $0 < \log(19.46\,\iota) < 3.15$, so $\theta \log c_0 \geq 2 + |\log(19.46\,\iota)|$. Third, $\Phi_{c_0}(\iota c_0^\theta) > 3.28 \cdot 10^{18} > 0$. Fourth, $\theta \iota c_0^\theta > 1.67 \cdot 10^{18}$, whereas $K_E \log c_0\,\big(2\log(19.46\,\iota c_0^\theta) + \theta \log c_0\big) < 5.78 \cdot 10^{16}$. These four values were verified in 256-bit interval arithmetic with outward rounding.

Hence Lemma 7.4 gives $\Phi_c(\iota c^{1/4}) > 0$. Since $\iota c^{1/4} \geq 1$, Proposition 7.3 with $u_0 = \iota c^{1/4}$ gives $2m < \iota c^{1/4}$, which contradicts the floor above. Therefore $c < 10^{75}$. □

The value 10^{75} is not the limit of this argument: the function $c \mapsto \Phi_c(2^{1/4} c^{1/4})$ changes sign near $\log_{10} c = 73.74$, so the same comparison gives $c < 10^{73.75}$. We keep 10^{75} because it is the upper end of the first window of the index caps.

7.2 Index caps on windows of c

Below 10^{75} we use the sharper lower bound of Mignotte and Voutier for linear forms in three logarithms (Theorem 7.6). It is quoted with its factorial term $\mathfrak{b}$ read from the definition: the displayed statement of Lemma 3.5(b) of [24] transposes two coefficients, as the proof of Theorem 7.6 explains. In Proposition 7.8 it is applied to Λ_x in the basis $(\alpha, D_\lambda, \beta/\alpha)$ rather than $(\alpha, \beta, D_\lambda)$. The reason is the unit β/α: its height is $\frac{1}{2}\log\beta$ (Lemma 4.2, item 3), but its logarithm is less

than $\log 2 + 4/c$ (item 1), so its parameter $(\rho-1)\log(\beta/\alpha) + 8\,\mathrm{h}(\beta/\alpha)$ in Theorem 7.6 is about $4\log\beta$, where β itself would need $(\rho+3)\log\beta$, that is $28\log\beta$ for the value $\rho = 25$ used there. The Liouville bound Lemma 7.7 serves one step of that proof: it shows that the two logarithms of the centred linear form in two logarithms have opposite signs.

Theorem 7.6. *Let $\eta_1, \eta_2, \eta_3 > 1$ be real algebraic numbers that are multiplicatively independent, put $\mathcal{D} = [\mathbb{Q}(\eta_1,\eta_2,\eta_3) : \mathbb{Q}]$, let b_1, b_2, b_3 be positive integers with $\gcd(b_1,b_2,b_3) = 1$, and*

$$\Lambda_{\mathrm{MV}} = b_1\log\eta_1 + b_2\log\eta_2 - b_3\log\eta_3, \qquad 0 < |\Lambda_{\mathrm{MV}}| < 2\pi/w,$$

where w is the largest order of a root of unity in $\mathbb{Q}(\eta_1,\eta_2,\eta_3)$. Let $K_0 \ge 3$, $\ell \ge 5$, R_{MV}, S, T be positive integers, put $N_* = K_0(K_0+1)\ell/2$, assume $R_{\mathrm{MV}}ST \ge N_*$, and put $g = \frac{1}{4} - \frac{N_*}{12R_{\mathrm{MV}}ST}$. Put $\delta_1 = \gcd(b_1,b_3)$, $\delta_2 = \gcd(b_2,b_3)$ and

$$\mathfrak{b} = \frac{(R_{\mathrm{MV}}-1)b_3 + (T-1)b_1}{2\delta_1} \cdot \frac{(S-1)b_3 + (T-1)b_2}{2\delta_2} \cdot \Big(\prod_{j=1}^{K_0-1} (j!)^{K_0-j}\Big)^{-\frac{12}{K_0(K_0-1)(K_0+1)}}.$$

Let $R_1, R_2, R_3, S_1, S_2, S_3, T_1, T_2, T_3$ be positive integers with $R_{\mathrm{MV}} > R_1+R_2+R_3$, $S > S_1+S_2+S_3$ and $T > T_1+T_2+T_3$. Let $\rho \ge 2$ be real, and let A_1, A_2, A_3 be real numbers with $A_i \ge (\rho-1)\log\eta_i + 2\mathcal{D}\,\mathrm{h}(\eta_i)$ (Definition 4.1), such that

$$\Big(\frac{K_0\ell}{2} + \frac{\ell}{2} - 0.37K_0 - 2\Big)\log\rho \ge (\mathcal{D}+1)\log N_* + g\ell\,(A_1R_{\mathrm{MV}} + A_2S + A_3T) + \frac{2\mathcal{D}(K_0-1)}{3}\log\mathfrak{b}.$$

Put $\mathcal{V} = \sqrt{(R_1+1)(S_1+1)(T_1+1)}$, and suppose that for some real $\chi > 0$

$$(R_1+1)(S_1+1)(T_1+1) > K_0\,\mathcal{M}, \qquad \mathcal{M} = \max\{R_1+S_1+1,\ S_1+T_1+1,\ R_1+T_1+1,\ \chi\mathcal{V}\},$$
$$\#\{\eta_1^{j_1}\eta_2^{j_2}\eta_3^{j_3} : 0 \le j_1 \le R_1,\ 0 \le j_2 \le S_1,\ 0 \le j_3 \le T_1\} > \ell,$$
$$\#\{\eta_1^{j_1}\eta_2^{j_2}\eta_3^{j_3} : 0 \le j_1 \le R_2,\ 0 \le j_2 \le S_2,\ 0 \le j_3 \le T_2\} > 2K_0\ell,$$
$$(R_2+1)(S_2+1)(T_2+1) > K_0^2, \qquad (R_3+1)(S_3+1)(T_3+1) > 3K_0^2\ell.$$

Then

$$\Lambda'_{\mathrm{MV}} = |\Lambda_{\mathrm{MV}}| \cdot \frac{\ell T\, e^{\ell T|\Lambda_{\mathrm{MV}}|/(2b_3)}}{2b_3} > \rho^{-K_0\ell},$$

or one of the following holds:

(C1) $b_1 \le \max\{R_1,R_2\}$, $b_2 \le \max\{S_1,S_2\}$ and $b_3 \le \max\{T_1,T_2\}$;

(C2) there are integers u_1, u_2, u_3 with $\gcd(u_1,u_2,u_3) = 1$ and $u_1b_1 + u_2b_2 + u_3b_3 = 0$, such that

$$|u_1| \le \frac{(S_1+1)(T_1+1)}{\mathcal{M} - \max\{S_1,T_1\}}, \qquad |u_2| \le \frac{(R_1+1)(T_1+1)}{\mathcal{M} - \max\{R_1,T_1\}}, \qquad |u_3| \le \frac{(R_1+1)(S_1+1)}{\mathcal{M} - \max\{R_1,S_1\}}.$$

Proof. This is [24, Theorem 2.1] in its real case (numbering of the arXiv version 3), with the conventions and notation of its Sections 2.1 and 2.2. The parameters written here K_0, ℓ, N_*, R_{MV}, A_i, δ_1, δ_2 are K, L, N, R, a_i, d_1, d_2 there, and $\mathcal{D}$ is the quotient $[\mathbb{Q}(\eta_1,\eta_2,\eta_3) : \mathbb{Q}]/[\mathbb{R}(\eta_1,\eta_2,\eta_3) : \mathbb{R}]$ of its Liouville inequality, which in the real case is the degree. The number $\mathfrak{b}$ is the quantity b of its definition (2.5), written out by means of (2.3) and (2.4), since $b'_3\eta_0 = \frac{(R_{\mathrm{MV}}-1)b_3+(T-1)b_1}{2\delta_1}$ and $b''_3\zeta_0 = \frac{(S-1)b_3+(T-1)b_2}{2\delta_2}$. For real $\eta_i > 1$ the lower bound for a_i in the source, $\rho|\log\eta_i| - \log|\eta_i| + 2\mathcal{D}\,\mathrm{h}(\eta_i)$, is the one stated here. Two remarks on the source. First, $\mathfrak{b}$ is to be read from (2.5): the displayed statement of its Lemma 3.5(b) transposes b_2 and b_3 in the second fraction, a misprint, as the last display of the proof of that lemma and the entries $\binom{s_jb''_3+t_jb''_2}{m_i}$ of its interpolation determinant show. Second, if $\mathbb{Q}(\eta_1,\eta_2,\eta_3)$ is real then $w = 2$, and the condition on Λ_{MV} reads $0 < |\Lambda_{\mathrm{MV}}| < \pi$. □

Lemma 7.7. *Let $\eta \neq 1$ be a positive real algebraic number with $[\mathbb{Q}(\eta) : \mathbb{Q}] \leq 4$. Then*

$$\log|\log\eta| > -4\,\mathrm{h}(\eta) - 4.$$

Proof. We first bound $|\eta - 1|$ from below by evaluating the primitive minimal polynomial of η at 1. Let $\mathcal{D} = [\mathbb{Q}(\eta) : \mathbb{Q}] \leq 4$ and let $P(X) = a_\eta \prod_{i=1}^{\mathcal{D}} (X - \eta_i) \in \mathbb{Z}[X]$ be the primitive minimal polynomial of η, with $a_\eta > 0$ and $\eta_1 = \eta$. By Definition 4.1, $a_\eta \prod_{i=1}^{\mathcal{D}} \max(1, |\eta_i|) = e^{\mathcal{D}\,\mathrm{h}(\eta)}$. Since P is irreducible and $\eta \neq 1$, the integer $P(1)$ is nonzero, so

$$1 \leq |P(1)| = a_\eta\,|1 - \eta| \prod_{i=2}^{\mathcal{D}} |1 - \eta_i| \leq |1 - \eta| \cdot a_\eta \prod_{i=2}^{\mathcal{D}} 2\max(1, |\eta_i|) \leq 2^{\mathcal{D}-1} e^{\mathcal{D}\,\mathrm{h}(\eta)}\,|\eta - 1|,$$

using $|1 - \eta_i| \leq 2\max(1, |\eta_i|)$ and $\max(1, |\eta|) \geq 1$. As $\mathcal{D} \leq 4$ and $\mathrm{h}(\eta) \geq 0$, this gives

$$\log|\eta - 1| \geq -4\,\mathrm{h}(\eta) - 3\log 2.$$

We now pass from $|\eta - 1|$ to $|\log\eta|$ in three cases. If $1 < \eta \leq 2$, then $\log\eta \geq \frac{\eta-1}{\eta} \geq \frac{\eta-1}{2}$, so $\log\log\eta \geq \log(\eta - 1) - \log 2 \geq -4\,\mathrm{h}(\eta) - 4\log 2 > -4\,\mathrm{h}(\eta) - 4$. If $0 < \eta < 1$, then $|\log\eta| = -\log\eta \geq 1 - \eta = |\eta - 1|$, so $\log|\log\eta| \geq -4\,\mathrm{h}(\eta) - 3\log 2 > -4\,\mathrm{h}(\eta) - 4$. If $\eta > 2$, then $\log|\log\eta| > \log\log 2 > -0.37 > -4 \geq -4\,\mathrm{h}(\eta) - 4$. This proves the bound in all cases. □

Proposition 7.8. *Let (λ, l, m, n) be the index system of an irregular extension d of an Euler triple $\{a, b, c\}$, and suppose that $c \geq 10^{48.6}$.*

1. *If $c < 10^{75}$, then $m < 7 \cdot 10^{12}$.*
2. *If $c < 10^{52}$, then $m < 3.45 \cdot 10^{12}$.*
3. *If $c < 10^{51}$, then $m < 1.1 \cdot 10^{12}$.*
4. *If $c < 10^{48.77}$, then $m < 10^{12}$.*

Proof. We apply the theorem of Mignotte and Voutier (Theorem 7.6) to the linear form Λ_x of Definition 2.16 in the basis $(\alpha, D_\lambda, \beta/\alpha)$, and exclude its exceptional alternative (C2) by a linear form in two logarithms centred at the relation it provides, together with Laurent's theorem (Theorem 4.3) applied separately for each denominator. The argument is the same in four rows, which differ only in their parameters; each row starts from the cap proved by the row before, and the first from the a priori bound (Proposition 7.3).

We first fix the parameters. Put $L_0 = 48.6\log 10$, $\rho = 25$, $M_{\mathrm{MV}} = \frac{5}{2}$, $\rho_+ = \rho + 3 = 28$, $\rho_- = \rho - 1 = 24$, and

	$U/\log 10$	Q_0	Q	χ	ℓ
row 1	75	$3.4 \cdot 10^{18}$	$1.4 \cdot 10^{13}$	13/10	320
row 2	52	$1.4 \cdot 10^{13}$	$6.9 \cdot 10^{12}$	13/10	312
row 3	51	$6.9 \cdot 10^{12}$	$2.2 \cdot 10^{12}$	3/5	198
row 4	48.77	$2.2 \cdot 10^{12}$	$2 \cdot 10^{12}$	1/2	196

In each row we assume $L_0 \le \log c < U$ and prove $2m < Q$; rows 1, 2, 3 and 4 prove items 1, 2, 3 and 4.

We next show $2m < Q_0$ in each row. In row 1, with Φ_c and K_E as in Convention 7.1, since $\log c < U$ and $\log(19.46\,Q_0) > 0$,

$$\Phi_c(Q_0) \ge Q_0 - 0.15 - K_E U^2 \log(19.46\,Q_0) > 0,$$

because $K_E U^2 \log(19.46\,Q_0) + 0.15 < 3.3535 \cdot 10^{18}$; so Proposition 7.3 with $u_0 = Q_0 \ge 1$ gives $2m < Q_0$. In rows 2, 3 and 4, Q_0 is the value of Q in rows 1, 2 and 3, whose windows contain the window of the row; so $2m < Q_0$ follows from those rows, which are proved first.

Suppose $2m \ge Q$; we derive a contradiction in each row. By item 4 of Lemma 2.18, $\Lambda_x < 4.01\,\beta^{-4m}$, and $\log 4.01 < 1.39$, so

$$\log \Lambda_x < -4m \log \beta + 1.39. \tag{1}$$

We next set up the linear form in three logarithms. By Definition 2.16, $\Lambda_x = 2l \log \alpha - 2m \log \beta + \log D_\lambda = (2l - 2m) \log \alpha + \log D_\lambda - 2m \log(\beta/\alpha)$, and $l > m$ by Lemma 2.14. We apply Theorem 7.6 with $(\eta_1, \eta_2, \eta_3) = (\alpha, D_\lambda, \beta/\alpha)$ and $(b_1, b_2, b_3) = (2l - 2m, 1, 2m)$. The b_i are positive integers with $\gcd(b_1, b_2, b_3) = 1$. By item 6 of Lemma 4.2, the η_i exceed 1 and are multiplicatively independent, and they generate the real biquadratic field $\mathcal{K}$ of item 2 (already α and $\beta = \alpha \cdot \beta/\alpha$ do), so $\mathcal{D} = 4$; as $\mathcal{K}$ is real, the condition on Λ_{MV} in Theorem 7.6 reads $0 < \Lambda_x < \pi$, which holds as $\Lambda_x < 1$ by item 4 of Lemma 2.18. Put

$$A_1 = \rho_+ \log \alpha, \qquad A_2 = 8 \log c + \rho_- \log 4, \qquad A_3 = \rho_+ \log \beta - \rho_- \log \alpha = 4 \log \beta + \rho_- \log(\beta/\alpha).$$

These are admissible: by item 3 of Lemma 4.2, $\mathrm{h}(\alpha) = \frac{1}{2} \log \alpha$ and $\mathrm{h}(\beta/\alpha) = \frac{1}{2} \log \beta$, so $A_1 = (\rho - 1) \log \alpha + 8\,\mathrm{h}(\alpha)$ and $A_3 = (\rho - 1) \log(\beta/\alpha) + 8\,\mathrm{h}(\beta/\alpha)$; and by item 4, $(\rho - 1) \log D_\lambda + 8\,\mathrm{h}(D_\lambda) < \rho_- \log 4 + 8 \log c = A_2$. Item 1 of Lemma 4.2 gives

$$A_1 > \frac{\rho_+ L_0}{2}, \qquad A_2 \ge 8L_0 + \rho_- \log 4, \qquad A_3 > 4 \log \beta > 2L_0 + 4 \log 2,$$

so $A_- := \min_i A_i > 2L_0 + 4 \log 2$ and $\Omega := A_1 A_2 A_3 > \Omega_-$, the product of these three lower bounds. Also $A_1 < A_1^+ := \rho_+(U - \log 2)$, $A_2 < A_2^+ := 8U + \rho_- \log 4$, and $A_1 + A_2 + A_3 = 4 \log \alpha + \rho_+ \log \beta + 8 \log c + \rho_- \log 4 < \Sigma_+ := (12 + \rho_+)U + \rho_- \log 4$.

We next bound the product Ω. Put $\varepsilon = 4 \cdot 10^{-48.6}$, so that $\log \beta - \log \alpha < \log 2 + \varepsilon$ by item 1 (as $4/c \le \varepsilon$). Then $(\log \alpha)^2 / \log \beta > (\log \alpha)^2 / (\log \alpha + \log 2 + \varepsilon) > \log \alpha - \log 2 - \varepsilon$, so $A_3 \log \alpha / \log \beta = \rho_+ \log \alpha - \rho_- (\log \alpha)^2 / \log \beta < 4 \log \alpha + \rho_- (\log 2 + \varepsilon) < 4 \log c + (\rho_- - 4) \log 2 + \rho_- \varepsilon$, using $\log \alpha < \log c - \log 2$. Hence, with $\Upsilon(Y) = \rho_+ \left(8Y + \rho_- \log 4\right) \left(4Y + (\rho_- - 4) \log 2 + \rho_- \varepsilon\right)$ for real $Y > 0$,

$$\frac{\Omega}{\log \beta} < \Upsilon(\log c) \le \Upsilon(U), \qquad \Omega < \Omega_+ := \Upsilon(U)\,U. \tag{2}$$

We now choose the remaining parameters of Theorem 7.6 and check its side conditions. Following Section 5.2 of [24], put $K_0 = \lfloor M_{\mathrm{MV}} \ell \Omega \rfloor$, $c_1 = (\chi M_{\mathrm{MV}} \ell)^{2/3}$, $c_2 = (M_{\mathrm{MV}} \ell)^{2/3}$, $c_3 = (3M_{\mathrm{MV}}^2)^{1/3} \ell$, $R_i = \lfloor c_i A_2 A_3 \rfloor$, $S_i = \lfloor c_i A_1 A_3 \rfloor$, $T_i = \lfloor c_i A_1 A_2 \rfloor$ for $i = 1, 2, 3$, $R_{\mathrm{MV}} = 1 + \sum R_i$, $S = 1 + \sum S_i$, $T = 1 + \sum T_i$, and $C_* = c_1 + c_2 + c_3$. Then $R_i + 1 > c_i A_2 A_3$, and similarly for S_i, T_i. The side checks $c_1^2 > 2M_{\mathrm{MV}} \ell / A_-$, $\chi \sqrt{c_1}\, A_- > 1$ and $M_{\mathrm{MV}} \Omega_- > 2$ hold in every row. First, $\mathcal{V}^2 = (R_1 + 1)(S_1 + 1)(T_1 + 1) > c_1^3 \Omega^2 = (\chi M_{\mathrm{MV}} \ell \Omega)^2 \ge (\chi K_0)^2$, so $\mathcal{V}^2 > K_0 \chi \mathcal{V}$; and

$$\begin{aligned} \frac{(R_1 + 1)(S_1 + 1)(T_1 + 1)}{R_1 + S_1 + 1} &> \frac{T_1 + 1}{(R_1 + 1)^{-1} + (S_1 + 1)^{-1}} > \frac{c_1^2 \Omega}{A_1^{-1} + A_2^{-1}} \\ &\ge \frac{c_1^2 A_- \Omega}{2} > M_{\mathrm{MV}} \ell \Omega \ge K_0, \end{aligned}$$

and likewise for the other two pairs; so $(R_1+1)(S_1+1)(T_1+1) > K_0\mathcal{M}$. By the multiplicative independence of the η_i, the two cardinalities in Theorem 7.6 equal $(R_1+1)(S_1+1)(T_1+1)$ and $(R_2+1)(S_2+1)(T_2+1)$; and $c_1^3\Omega^2 > \ell$, $c_2^3\Omega^2 = (M_{\mathrm{MV}}\ell\Omega)^2 > \max(2K_0\ell, K_0^2)$ (as $M_{\mathrm{MV}}\Omega > 2$), $c_3^3\Omega^2 = 3M_{\mathrm{MV}}^2\ell^3\Omega^2 \geq 3K_0^2\ell$ give the remaining four conditions. Finally $R_{\mathrm{MV}}ST > c_3^3\Omega^2 > N_* = K_0(K_0+1)\ell/2$, $K_0 \geq 3$ and $\ell \geq 5$.

We next bound the factorial term $\mathfrak{b}$ of Theorem 7.6. Here $\delta_1 = \gcd(2l-2m, 2m) \geq 1$ and $\delta_2 = \gcd(1, 2m) = 1$, and the last factor of $\mathfrak{b}$ is at most $e^{11/3}K_0^{-2}$ by [24, Lemma 3.5(a)]. With $(b_1, b_2, b_3) = (2l-2m, 1, 2m)$ this gives

$$\log\mathfrak{b} \leq \log\frac{2(R_{\mathrm{MV}}-1)m + (T-1)(2l-2m)}{2} + \log\frac{2(S-1)m+(T-1)}{2} - 2\log K_0 + \frac{11}{3}.$$

Since $R_{\mathrm{MV}} - 1 \leq C_*A_2A_3$, $S-1 \leq C_*A_1A_3$ and $T-1 \leq C_*A_1A_2$, the two numerators are at most $C_*\Omega\bigl(\frac{2m}{A_1} + \frac{2l-2m}{A_3}\bigr)$ and $C_*\Omega\bigl(\frac{2m}{A_2} + \frac{1}{A_3}\bigr)$. As $l\log\alpha < m\log\beta$ (item 1 of Lemma 2.18), $2l-2m < 2m\log(\beta/\alpha)/\log\alpha$; with $A_3 > 4\log\beta$, $\log\alpha > \frac12\log c$, $\log\beta > \frac12\log c$ and $2m < Q_0$,

$$\frac{2m}{A_1} + \frac{2l-2m}{A_3} < \frac{2m}{\log\alpha}\Bigl(\frac{1}{\rho_+} + \frac{\log 2+\varepsilon}{4\log\beta}\Bigr) < \frac{2Q_0}{L_0}\Bigl(\frac{1}{\rho_+} + \frac{\log 2+\varepsilon}{2L_0}\Bigr) =: \mathcal{N}_1,$$
$$\frac{2m}{A_2} + \frac{1}{A_3} < \frac{Q_0}{8L_0 + \rho_-\log 4} + \frac{1}{2L_0 + 4\log 2} =: \mathcal{N}_2.$$

With $K_0 \geq M_{\mathrm{MV}}\ell\Omega - 1$ we obtain

$$\log\mathfrak{b} < \mathcal{B} := 2\log\frac{C_*}{M_{\mathrm{MV}}\ell} + \log\frac{\mathcal{N}_1\mathcal{N}_2}{4} + \frac{11}{3} - 2\log\Bigl(1 - \frac{1}{M_{\mathrm{MV}}\ell\Omega_-}\Bigr).$$

We next reduce the main condition of Theorem 7.6 to one numerical inequality. With $\mathcal{D} = 4$ it reads $\bigl(\frac{K_0\ell}{2} + \frac{\ell}{2} - 0.37K_0 - 2\bigr)\log\rho \geq 5\log N_* + g\ell(A_1R_{\mathrm{MV}} + A_2S + A_3T) + \frac{8(K_0-1)}{3}\log\mathfrak{b}$. Divide by K_0. The left side becomes at least $(\frac{\ell}{2} - 0.37)\log\rho$, as $\ell \geq 4$. On the right, $\frac{5\log N_*}{K_0} < \frac{5\log N_+}{K_-}$ with $K_- = M_{\mathrm{MV}}\ell\Omega_- - 1$, $K_+ = M_{\mathrm{MV}}\ell\Omega_+$ and $N_+ = K_+(K_+ + 1)\ell/2$; next $g \leq \frac14$ and $A_1R_{\mathrm{MV}} + A_2S + A_3T \leq 3C_*\Omega + \Sigma_+$, and $(3C_*\Omega + \Sigma_+)/(M_{\mathrm{MV}}\ell\Omega - 1)$ decreases with Ω; finally $\frac{8(K_0-1)}{3K_0}\log\mathfrak{b} < \frac83\mathcal{B}$. Hence the main condition follows from

$$\Bigl(\frac{\ell}{2} - 0.37\Bigr)\log\rho > \frac{5\log N_+}{K_-} + \frac{\ell}{4}\cdot\frac{3C_*\Omega_- + \Sigma_+}{M_{\mathrm{MV}}\ell\Omega_- - 1} + \frac83\mathcal{B}, \tag{3}$$

which holds in every row, with the margins shown in the table below.

We now exclude the main alternative of Theorem 7.6. Put $T_0 = \ell\bigl(1 + C_*A_1^+A_2^+\bigr)$, so that $\ell T \leq T_0$; in every row $T_0 < Q/2$. As $2m \geq Q$ and $\Lambda_x < 1$, $\Lambda'_{\mathrm{MV}} = \Lambda_x\frac{\ell T}{4m}e^{\ell T\Lambda_x/(4m)} < \frac14 e^{1/4}\Lambda_x < \Lambda_x$. The inequality $\Lambda'_{\mathrm{MV}} > \rho^{-K_0\ell}$ then gives $\log\Lambda_x > -M_{\mathrm{MV}}\ell^2\Omega\log\rho$, and with (1), (2) and $\log\beta > \frac{L_0}{2} + \log 2$,

$$2m < \frac{M_{\mathrm{MV}}\ell^2\log\rho}{2}\cdot\frac{\Omega}{\log\beta} + \frac{1.39}{2\log\beta} < \frac{M_{\mathrm{MV}}\ell^2\log\rho}{2}\,\Upsilon(U) + \frac{1.39}{L_0 + 2\log 2} =: \mathrm{cap}.$$

In every row $\mathrm{cap} < Q$, which contradicts $2m \geq Q$.

Alternative (C1) gives $2m = b_3 \leq \max(T_1, T_2) \leq \max(c_1, c_2)\,A_1A_2 < \max(c_1, c_2)\,A_1^+A_2^+$, and the last number is below $7\cdot 10^8 < Q$ in every row; this is impossible.

It remains to exclude alternative (C2); this is the main step of the proof. Let u_1, u_2, u_3 be the integers of (C2): $\gcd(u_1, u_2, u_3) = 1$, $u_1(2l-2m) + u_2 + 2u_3m = 0$, $|u_1| \leq \frac{(S_1+1)(T_1+1)}{\mathcal{M} - \max(S_1, T_1)}$, and the

two analogous bounds hold. Since $\mathcal{M} \geq \chi\mathcal{V} > \chi c_1^{3/2}\Omega$, $(S_1+1)(T_1+1) \leq c_1^2 A_1^2 A_2 A_3\big(1+\frac{1}{c_1 A_-^2}\big)^2$ and $\max(S_1,T_1) \leq c_1 A_1 \max(A_2,A_3)$, and similarly for u_2, u_3, we get $|u_i| \leq F A_i$ with

$$F = \frac{\sqrt{c_1}}{\chi}\,\frac{\big(1+1/(c_1 A_-^2)\big)^2}{1-1/(\chi\sqrt{c_1}\,A_-)}.$$

If $u_1 = 0$, then $u_3 \neq 0$ by coprimality and $2m \leq |u_2| < F A_2^+$; in every row $F A_2^+ < Q$, which is impossible. So $u_1 \neq 0$; let $\mathfrak{d} = \gcd(u_1, u_1 - u_3)$, which divides u_2, and put $q = |u_1|/\mathfrak{d}$, $\mathfrak{a} = \operatorname{sgn}(u_1)(u_1-u_3)/\mathfrak{d}$ and $C_{\mathrm{rel}} = -\operatorname{sgn}(u_1)u_2/\mathfrak{d}$. Then

$$2\mathfrak{a}m - 2ql + C_{\mathrm{rel}} = 0, \qquad \gcd(\mathfrak{a}, q) = 1,$$
$$1 \leq q \leq q_{\max} := \lfloor F A_1^+ \rfloor, \qquad |C_{\mathrm{rel}}| \leq C_{\max} := \lfloor F A_2^+ \rfloor,$$

and $\mathfrak{a} > 0$ because $2\mathfrak{a}m = 2ql - C_{\mathrm{rel}} \geq 2l - |C_{\mathrm{rel}}| > 0$.

We rewrite $-\Lambda_x$ as a linear form in two logarithms, centred at this relation. Choose $p_0 \in \mathbb{Z}$ with $|p_0| \leq q/2$ and $\mathfrak{a}p_0 \equiv -C_{\mathrm{rel}} \pmod q$, and put $k_0 = (\mathfrak{a}p_0 + C_{\mathrm{rel}})/q$ and $\mathfrak{t} = (2m - p_0)/q$; these are integers, $\mathfrak{t} > 0$ and $2l = k_0 + \mathfrak{a}\mathfrak{t}$. With

$$\zeta = \beta^q \alpha^{-\mathfrak{a}}, \qquad \xi = D_\lambda^{-1}\beta^{p_0}\alpha^{-k_0},$$

one has exactly $-\Lambda_x = \mathfrak{t}\log\zeta + \log\xi$, $\log\zeta = \frac{C_{\mathrm{rel}}\log\alpha + q\log D_\lambda - q\Lambda_x}{2m}$ and $\log\xi = \frac{p_0}{q}\log\zeta - \frac{C_{\mathrm{rel}}\log\alpha}{q} - \log D_\lambda$. Using $\log\alpha < \log c < U$ (item 1 of Lemma 4.2), $0 < \Lambda_x < \log D_\lambda < \log 4$ and $\mathrm{h}(D_\lambda) < \log c < U$ (item 4 of Lemma 2.18 and item 4 of Lemma 4.2), $2m \geq Q$, the height formula of item 3 of Lemma 4.2, $\mathfrak{a}\log\alpha = q\log\beta - \log\zeta$ and $|k_0| \leq \frac{\mathfrak{a}}{2} + \frac{|C_{\mathrm{rel}}|}{q}$,

$$|\log\zeta| < Z_q := \frac{C_{\max}U + q\log 4}{Q}, \qquad |\log\xi| < X_q := \log 4 + \frac{Z_q}{2} + \frac{C_{\max}U}{q}, \qquad \mathfrak{t} < \mathfrak{t}_q := \frac{Q_0}{q} + \frac{1}{2},$$

and $\mathrm{h}(\zeta) = \frac{1}{2}\max(q\log\beta, \mathfrak{a}\log\alpha) \leq H_\zeta(\log\beta)$ and $\mathrm{h}(\xi) \leq H_\xi(\log\beta)$, where for real Y

$$H_\zeta(Y) = \tfrac{1}{2}(qY + Z_q), \qquad H_\xi(Y) = U + \frac{qY + Z_q}{4} + \frac{C_{\max}U}{2q};$$

both increase with Y. By item 2 of Lemma 4.2, the four embeddings of $\mathcal{K}$ send the unit ζ to the four numbers $\beta^{\pm q}\alpha^{\pm\mathfrak{a}}$, which are distinct by item 6, so $\zeta \neq 1$ generates $\mathcal{K}$; and $N_{\mathcal{K}/\mathbb{Q}}(\xi) = N_{\mathcal{K}/\mathbb{Q}}(D_\lambda)^{-1} \neq \pm 1$ by item 4, while units have norm ± 1, so ζ and ξ are multiplicatively independent. If $\log\zeta$ and $\log\xi$ had the same sign, then $\Lambda_x \geq |\log\xi|$, and Lemma 7.7, applied to the positive number $\xi \neq 1$ of degree at most four, would give $\log\Lambda_x > -4H_\xi(\log\beta) - 4 \geq -4H_\xi(U) - 4$; but in every row $4H_\xi(U) + 4 < 2Q(\frac{L_0}{2} + \log 2) - 1.39$ for every integer $1 \leq q \leq q_{\max}$, which contradicts (1). So the two logarithms have opposite signs. Replacing ζ or ξ by its inverse, $\Lambda_x = b_2\log\eta_2 - b_1\log\eta_1$ with $\{\eta_1,\eta_2\} = \{\zeta^{\pm1}, \xi^{\pm1}\}$ both greater than 1, the coefficient $\mathfrak{t}$ on the number from ζ and 1 on the number from ξ.

We finally apply Theorem 4.3 separately for each denominator q. Put $B^- = \frac{L_0}{2} + \log 2$ and $B^+ = U$, and split $[B^-, B^+]$, which contains $\log\beta$, into sixteen equal subintervals $[B_j, B_{j+1}]$, $0 \leq j \leq 15$. For fixed q and j with $\log\beta \in [B_j, B_{j+1}]$, apply Theorem 4.3 with $\mathcal{D} = 4$, $\rho = \rho_q := q+2$, $\mu = 0.63$, $\sigma_L = \frac{1+2\mu-\mu^2}{2}$, $\lambda_L = \sigma_L\log\rho_q$, with the numbers $A_\zeta \geq 8H_\zeta(B_{j+1}) + (\rho_q - 1)Z_q + 1$ and $A_\xi \geq 8H_\xi(B_{j+1}) + (\rho_q - 1)X_q + 1$ in the roles of the A_i of the numbers coming from ζ and ξ, and with

$$h_L \geq \max\Big\{4\Big(\log\Big(\frac{1}{A_\zeta} + \frac{\mathfrak{t}_q}{A_\xi}\Big) + \log\lambda_L + 1.75\Big) + 0.06,\ \lambda_L,\ 2\log 2\Big\},$$

each taken as the upper endpoint of its interval enclosure. These choices are admissible, since $\mathrm{h}(\eta^{-1}) = \mathrm{h}(\eta)$ and $\mathfrak{t} < \mathfrak{t}_q$. With $\mathcal{H}, \omega_L, \theta_L, \mathcal{C}, \mathcal{C}'$ as in Theorem 4.3 (for $A_1A_2 = A_\zeta A_\xi$), the theorem gives $\log \Lambda_x \geq -E_{q,j}$, where

$$E_{q,j} = \mathcal{C}(h_L + \log \rho_q)^2 A_\zeta A_\xi + \sqrt{\omega_L \theta_L}\,(h_L + \log \rho_q) + \log\bigl(\mathcal{C}'(h_L + \log \rho_q)^2 A_\zeta A_\xi\bigr).$$

For every integer $1 \leq q \leq q_{\max}$ and every j, in every row, $A_\zeta A_\xi > \lambda_L^2$ and $E_{q,j} < 2QB_j - 1.39$. Since $4m \log \beta \geq 2QB_j$, this contradicts (1).

The numerical values used above were computed in interval arithmetic of at least 160 bits with outward rounding, with A_- replaced by its lower bound $2L_0 + 4\log 2$ in the side checks and in F, which is legitimate because the side checks hold a fortiori and F decreases as A_- grows; each entry is an endpoint of an enclosure.

	$\Upsilon(U)/U^2$	$\mathcal{B}$	margin of (3)	cap	T_0	$(q_{\max}, C_{\max})$
row 1	< 935.993	< 74.037	> 4.712	$< 1.1502 \cdot 10^{13}$	$< 2.266 \cdot 10^{12}$	$(37546, 11030)$
row 2	< 953.96	< 49.240	> 65.28	$< 5.3567 \cdot 10^{12}$	$< 1.0458 \cdot 10^{12}$	$(25767, 7662)$
row 3	< 955.12	< 47.791	> 0.1046	$< 2.0777 \cdot 10^{12}$	$< 3.986 \cdot 10^{11}$	$(36387, 10828)$
row 4	< 957.86	< 45.490	> 6.351	$< 1.8671 \cdot 10^{12}$	$< 3.550 \cdot 10^{11}$	$(39162, 11675)$

The largest ratio $E_{q,j}/(2QB_j - 1.39)$ is below 0.8476, 0.1490, 0.6476, 0.5902 in rows 1 to 4, and occurs at $q = q_{\max}$, $j = 15$. In every row the side checks hold, the bound in (C1) is below $7 \cdot 10^8$, $FA_2^+ < Q$, and $H_\xi(U) < 1.63 \cdot 10^6$ for $1 \leq q \leq q_{\max}$.

All alternatives of Theorem 7.6 are excluded, so $2m < Q$ in each row. Rows 1, 2, 3 and 4 give $2m < 1.4 \cdot 10^{13}$, $2m < 6.9 \cdot 10^{12}$, $2m < 2.2 \cdot 10^{12}$ and $2m < 2 \cdot 10^{12}$, which are items 1, 2, 3 and 4.

□

Theorem 7.9. *Let $\{a, b, c, d\}$ be a Diophantine quadruple with $a < b < c < d$ and $c = a + b + 2\sqrt{ab+1}$. If $d \neq d_+(a, b, c)$, then $c < 4 \cdot 10^{48}$.*

Proof. The proof is a descent: starting from $c < 10^{75}$, each index cap of Proposition 7.8 gives, through the quartic index floor (Theorem 3.6), a smaller bound for c, until $c < 4 \cdot 10^{48}$.

We first put the hypotheses in the language of index systems. Since $\{a, b, c, d\}$ is a Diophantine quadruple, $ab + 1$ is a square, so $r = \sqrt{ab+1}$ is a positive integer and $c = a + b + 2r$: the set $\{a, b, c\}$ is an Euler triple (Definition 2.3). It is a Diophantine triple and $d > c$, so d is an extension of $\{a, b, c\}$, irregular because $d \neq d_+(a, b, c)$ (Definition 2.2). Let (λ, l, m, n) be its index system (Proposition 2.11).

We next record the form in which the floor is used. By Theorem 3.6, $c < 4m^2(m + \lambda)^2 \leq 4m^2(m + 1)^2$. Hence, for every positive integer Q,

$$m < Q \implies c < 4(Q - 1)^2 Q^2 < 4Q^4, \tag{1}$$

since then $m \leq Q - 1$ and $m(m + 1) \leq (Q - 1)Q$.

We now descend. By Proposition 7.5, $c < 10^{75}$. If $c < 10^{48.6}$, then $c < 4 \cdot 10^{48}$, as $10^{0.6} < 3.99$. Let $c \geq 10^{48.6}$. Item 1 of Proposition 7.8 gives $m < 7 \cdot 10^{12}$, so by (1)

$$c < 4\,(7 \cdot 10^{12})^4 = 9.604 \cdot 10^{51} < 10^{52}.$$

Item 2 of Proposition 7.8 now gives $m < 3.45 \cdot 10^{12}$, so by (1)

$$c < 4\,(3.45 \cdot 10^{12})^4 < 10^{51}.$$

Item 3 of Proposition 7.8 now gives $m < 1.1 \cdot 10^{12}$, so by (1)

$$c < 4\,(1.1 \cdot 10^{12})^4 < 10^{48.77}.$$

Item 4 of Proposition 7.8 now gives $m < 10^{12}$, and (1) gives

$$c < 4\,(10^{12} - 1)^2 \cdot 10^{24} < 4 \cdot 10^{48}.$$

Here $10^{0.6} < 3.99$ and $4\,(1.1 \cdot 10^{12})^4 < 10^{48.77}$ were verified in interval arithmetic with outward rounding; the other three comparisons are exact integer comparisons.

□

Every step of this descent uses the clause $c < 4m^2(m+\lambda)^2$ of the quartic floor, not only $c < 8m^4$. From $m < Q$ the weaker floor gives only $c < 8(Q-1)^4$, which for $Q = 7 \cdot 10^{12}$, $3.45 \cdot 10^{12}$, $1.1 \cdot 10^{12}$ and 10^{12} exceeds 10^{52}, 10^{51}, $10^{48.77}$ and $4 \cdot 10^{48}$, respectively; so none of the four steps would close, and the last would give only $c < 8 \cdot 10^{48}$. The effective bound is used once more, in Section 8, to confine the family with $K = 1$ to finitely many triples.

8 Families of Euler triples that extend only regularly

We apply the pair-coordinate criterion (Theorem 5.19), the coprime divisors (Theorem 6.3) and the effective bound (Theorem 7.9) to two families of Euler triples: the three-parameter Fibonacci family of Cipu, Fujita and Mignotte [10] (Subsection 8.1), and the triples with two elements in a fixed ratio (Subsection 8.2). The following table lists the families of Euler triples whose regularity follows from our results, with what was known before.

Family	Previously known	This paper
three-parameter family of [10], $\nu A \geq 2$	$K \geq 165F_\nu A$; the cases $\nu = 1$, $A = 1$ and $\nu, A \leq 10$ [10]	$K \geq 643$; $K \geq 128$ if $c \geq 4.5 \cdot 10^{12}$ (Corollary 8.3)
the same with $K = 1$, $A \in \{2, 3\}$	$\nu \leq 10$ [10]; for $(A, \varepsilon) = (3, -1)$, $\{F_{2\nu+2}, F_{2\nu+4}, F_{2\nu+6}\}$ [12]	all $\nu \geq 2$ (Theorem 8.4)
two elements in ratio $j : k$	$b/a \in \{2, 3, 6\}$ via [1]; $\{P_{2k}, P_{2k+2}, 2P_{2k+2}\}$ [2]	all $j : k$ with $jk \leq 300$ (Theorem 8.7)
b far from or close to a	$b < a + 4\sqrt{a}$ [17]	$b \geq 3355^2 a$ or $\sqrt{ac} \geq 3075(b-a)$ (Theorem 4.5)

Here P_k denotes the k-th Pell number. Any further family all of whose members satisfy $b \geq 3355^2 a$, or $\sqrt{ac} \geq 3075(b-a)$, is covered by Theorem 4.5 directly. The proofs are completed in the appendices: Appendix A treats the range $643 \leq K \leq 2401$ of the three-parameter family, and Appendix B gives the reduction that settles the finitely many single triples left below the analytic bounds.

8.1 The three-parameter Fibonacci family

Convention 8.1. The **three-parameter Fibonacci family** is the family of [10] in the case $|\varepsilon| = 1$, defined as follows. Let $F_{-1} = 1$, $F_0 = 0$ and $F_{k+2} = F_{k+1} + F_k$. For integers $\nu \geq 1$, $A \geq 1$, $K \geq 1$ and a sign $\varepsilon \in \{-1, 1\}$ put, for $k \geq 0$,

$$\phi_k = F_k A + F_{k-1}, \qquad \psi_k = \phi_k K + 2\varepsilon F_k, \qquad f_k = \phi_k \psi_k,$$

and $X = F_\nu A$. The quadruple (ν, A, K, ε) is a **parameter point**, and the set $\{f_\nu, f_{\nu+1}, f_{\nu+2}\}$ is its **family triple**; when the family triple is an Euler triple, its elements are $a = f_\nu$, $b = f_{\nu+1}$, $c = f_{\nu+2}$.

Lemma 8.2. *Let (ν, A, K, ε) be a parameter point (Convention 8.1), and put*

$$r = \phi_\nu \phi_{\nu+1} K + \varepsilon\big(F_\nu \phi_{\nu+1} + F_{\nu+1}\phi_\nu\big).$$

1. *$f_\nu f_{\nu+1} + 1 = r^2$ and $f_{\nu+2} = f_\nu + f_{\nu+1} + 2r$.*
2. *If $K \geq 3$, or if $K = 1$, $A \geq 2$ and $\nu \geq 2$, then $0 < f_\nu < f_{\nu+1}$ and $r > 0$. Hence the family triple $\{a, b, c\}$ is an Euler triple with root r, and $(\phi_\nu, \psi_\nu, \phi_{\nu+1}, \psi_{\nu+1})$ is a pair representation of it of sign $\varepsilon(-1)^\nu$, with pair coordinates $(p_3, q_3) = (\phi_{\nu+2}, \psi_{\nu+2})$.*
3. *If $K \geq 3$, then this pair representation satisfies $p_1 q_3 \geq \frac{K-2}{3}\, p_3^2$.*

Proof. We first record an identity for a symmetric bilinear form. For $\xi = (\xi_1, \xi_2)$ and $\eta = (\eta_1, \eta_2)$ in $\mathbb{Z}^2$ put

$$\langle \xi, \eta \rangle = K\xi_1\eta_1 + \varepsilon(\xi_1\eta_2 + \xi_2\eta_1), \qquad [\xi, \eta] = \xi_1\eta_2 - \xi_2\eta_1.$$

Since $\varepsilon^2 = 1$,

$$\langle \xi, \eta \rangle^2 - \langle \xi, \xi \rangle \langle \eta, \eta \rangle = [\xi, \eta]^2.$$

We next prove item 1. Put $\mathbf{e}_k = (\phi_k, F_k)$ for $k \geq 0$. Since $F_{j+2} = F_{j+1} + F_j$ for $j \geq -1$, we have $\phi_{k+2} = \phi_{k+1} + \phi_k$, hence $\mathbf{e}_{k+2} = \mathbf{e}_{k+1} + \mathbf{e}_k$ and $\psi_{k+2} = \psi_{k+1} + \psi_k$, for $k \geq 0$. Moreover $f_k = \phi_k\psi_k = \langle \mathbf{e}_k, \mathbf{e}_k \rangle$ and $r = \langle \mathbf{e}_\nu, \mathbf{e}_{\nu+1} \rangle$. By Cassini's identity $F_{k-1}F_{k+1} - F_k^2 = (-1)^k$, valid for $k \geq 0$ with $F_{-1} = 1$,

$$[\mathbf{e}_k, \mathbf{e}_{k+1}] = (F_k A + F_{k-1})F_{k+1} - F_k(F_{k+1}A + F_k) = (-1)^k \qquad (k \geq 0).$$

So the identity above gives $r^2 - f_\nu f_{\nu+1} = 1$, and bilinearity gives $f_{\nu+2} = \langle \mathbf{e}_\nu + \mathbf{e}_{\nu+1}, \mathbf{e}_\nu + \mathbf{e}_{\nu+1} \rangle = f_\nu + f_{\nu+1} + 2r$.

We now show that $\langle \mathbf{e}_k, \mathbf{e}_j \rangle > 0$ for the pairs of indices needed below. For $k \geq 0$ we have $F_k \geq 0$, $\phi_k \geq 1$ and $F_k \leq \phi_k$, since $\phi_0 = 1$, $\phi_1 = A$ and $\phi_k = F_k A + F_{k-1} \geq F_k$ for $k \geq 1$. If $K \geq 3$, then for all $k, j \geq 0$

$$\langle \mathbf{e}_k, \mathbf{e}_j \rangle \geq K\phi_k\phi_j - (F_k\phi_j + F_j\phi_k) \geq \phi_k\phi_j(K - 2) > 0.$$

Let $K = 1$ and $A \geq 2$. For $k \geq 0$, $\phi_k - F_k = (A-1)F_k + F_{k-1} \geq F_k + F_{k-1} = F_{k+1}$. If $\varepsilon = 1$, then $\langle \mathbf{e}_k, \mathbf{e}_j \rangle \geq \phi_k\phi_j \geq 1$ for $k, j \geq 0$. If $\varepsilon = -1$, then for $k, j \geq 0$

$$\langle \mathbf{e}_k, \mathbf{e}_j \rangle = (\phi_k - F_k)(\phi_j - F_j) - F_kF_j \geq F_{k+1}F_{j+1} - F_kF_j,$$

and the right side is positive unless $k = j = 1$, because $F_{i+1} \geq 1$ and $F_{i+1} \geq F_i$ for $i \geq 0$, with equality in the second only for $i = 1$. So, for $K = 1$ and $A \geq 2$, $\langle \mathbf{e}_k, \mathbf{e}_j \rangle > 0$ for all $k, j \geq 0$ with $(k, j) \neq (1, 1)$.

We next prove item 2. The pairs (ν, ν), $(\nu+1, \nu+1)$, $(\nu, \nu+1)$ and $(\nu-1, \nu+2)$ have nonnegative entries, as $\nu \geq 1$, and none of them is $(1, 1)$ when $\nu \geq 2$; so under either hypothesis the previous paragraph gives $f_\nu > 0$, $f_{\nu+1} > 0$, $r > 0$ and, since $\mathbf{e}_{\nu+1} - \mathbf{e}_\nu = \mathbf{e}_{\nu-1}$ and $\mathbf{e}_{\nu+1} + \mathbf{e}_\nu = \mathbf{e}_{\nu+2}$,

$$f_{\nu+1} - f_\nu = \langle \mathbf{e}_{\nu+1} - \mathbf{e}_\nu, \mathbf{e}_{\nu+1} + \mathbf{e}_\nu \rangle = \langle \mathbf{e}_{\nu-1}, \mathbf{e}_{\nu+2} \rangle > 0.$$

By item 1, $f_\nu f_{\nu+1}+1=r^2$ with r a positive integer and $f_{\nu+2}=f_\nu+f_{\nu+1}+2r>f_{\nu+1}$; so $\{a,b,c\}$ is an Euler triple with root r. Put $(p_1,q_1,p_2,q_2)=(\phi_\nu,\psi_\nu,\phi_{\nu+1},\psi_{\nu+1})$. These are positive integers, since $\phi_\nu,\phi_{\nu+1}\geq 1$ and $\psi_\nu=f_\nu/\phi_\nu$, $\psi_{\nu+1}=f_{\nu+1}/\phi_{\nu+1}$ are positive. We have $a=p_1q_1$, $b=p_2q_2$ and

$$p_1q_2-p_2q_1=2\varepsilon\big(\phi_\nu F_{\nu+1}-\phi_{\nu+1}F_\nu\big)=2\varepsilon[\mathbf{e}_\nu,\mathbf{e}_{\nu+1}]=2\varepsilon(-1)^\nu,$$

so (p_1,q_1,p_2,q_2) is a pair representation of sign $\varepsilon(-1)^\nu$. Its pair coordinates are $p_3=\phi_\nu+\phi_{\nu+1}=\phi_{\nu+2}$ and $q_3=\psi_\nu+\psi_{\nu+1}=\psi_{\nu+2}$.

We finally prove item 3. As $K\geq 3$, item 2 applies. Moreover $\phi_{\nu-1}\leq\phi_\nu$: for $\nu=1$ this is $1\leq A$, and for $\nu\geq 2$, $\phi_\nu-\phi_{\nu-1}=\phi_{\nu-2}\geq 1$. Hence $\phi_{\nu+2}=2\phi_\nu+\phi_{\nu-1}\leq 3\phi_\nu$, and since $F_{\nu+2}\leq\phi_{\nu+2}$,

$$p_1q_3=\phi_\nu\big(\phi_{\nu+2}K+2\varepsilon F_{\nu+2}\big)\geq\phi_\nu\phi_{\nu+2}(K-2)\geq\frac{K-2}{3}\,\phi_{\nu+2}^2=\frac{K-2}{3}\,p_3^2.$$

□

Item 3 is the link with the pair-coordinate criterion: in the family, its hypothesis on p_1q_3/p_3^2 becomes a condition on K alone. The proof of the next corollary takes the range $643\leq K\leq 2401$ from Appendix A.

Corollary 8.3. *Let (ν,A,K,ε) be a parameter point of the three-parameter Fibonacci family with $\nu A\geq 2$, and let $\{a,b,c\}$ be its family triple. If*

$$K\geq 643,\qquad\text{or}\qquad K\geq 128\ \text{ and }\ c\geq 4.5\cdot 10^{12},$$

then $\{a,b,c\}$ has no irregular extension.

Proof. Under either hypothesis $K\geq 128$, so by Lemma 8.2, items 2 and 3, $\{a,b,c\}$ is an Euler triple with a pair representation satisfying $p_1q_3\geq\frac{K-2}{3}\,p_3^2$. Hence $p_1q_3\geq 42\,p_3^2$, and $p_1q_3\geq 800\,p_3^2$ if $K\geq 2402$; so, by Theorem 5.19, $\{a,b,c\}$ has no irregular extension if $K\geq 2402$ (first case) or if $c\geq 4.5\cdot 10^{12}$ (second case). Otherwise $643\leq K\leq 2401$, and the claim is Theorem A.5. □

For $K=1$ item 3 of Lemma 8.2 does not apply, and the next theorem is proved through the effective bound instead: together with $b>4000$, it confines ν, for each of the four pairs (A,ε), to a finite range, whose 427 triples are settled by the reduction of Appendix B.

Theorem 8.4. *Let $A\in\{2,3\}$, $\varepsilon\in\{-1,1\}$ and $\nu\geq 2$, and let $\{a,b,c\}$ be the family triple of the parameter point $(\nu,A,1,\varepsilon)$, that is,*

$$a=\phi_\nu(\phi_\nu+2\varepsilon F_\nu),\qquad b=\phi_{\nu+1}(\phi_{\nu+1}+2\varepsilon F_{\nu+1}),\qquad c=\phi_{\nu+2}(\phi_{\nu+2}+2\varepsilon F_{\nu+2}),$$

with $\phi_k=F_{k+2}$ if $A=2$ and $\phi_k=L_{k+1}$ if $A=3$, where L_k denotes the k-th Lucas number. Then $\{a,b,c\}$ is an Euler triple, and it has no irregular extension.

Proof. For $(A,\varepsilon)=(3,-1)$ one has $\phi_k-2F_k=L_{k+1}-2F_k=F_{k+1}$ and $L_{k+1}F_{k+1}=F_{2k+2}$, so the family triples are the Hoggatt–Bergum triples $\{F_{2\nu+2},F_{2\nu+4},F_{2\nu+6}\}$ (with $k=\nu+1$); for them the theorem is contained in Dujella's theorem [12]: if $\{F_{2k},F_{2k+2},F_{2k+4},d\}$ is a Diophantine quadruple, then $d=4F_{2k+1}F_{2k+2}F_{2k+3}$, which is $d_+(F_{2k},F_{2k+2},F_{2k+4})$. Filipin, Fujita and Togbé [17] proved the stronger statement that every Diophantine quadruple containing the pair $\{F_{2k},F_{2k+2}\}$ is regular. For $2\leq\nu\leq 10$ the theorem is contained in the result of Cipu, Fujita

and Mignotte [10] that the family triples with $1 \le \nu \le 10$ and $1 \le A \le 10$ have no irregular extension, for every K. The argument below treats the four cases and every $\nu \ge 2$ together.

We first record the Euler property and a monotonicity. By Lemma 8.2, item 2 (with $K = 1$, $A \ge 2$, $\nu \ge 2$), $\{a, b, c\}$ is an Euler triple. The same item, applied to every parameter point $(k, A, 1, \varepsilon)$ with $k \ge 2$, gives $f_k < f_{k+1}$; so $(f_k)_{k\ge 2}$ is strictly increasing, and $b = f_{\nu+1}$ and $c = f_{\nu+2}$ increase with ν.

Suppose that $\{a, b, c\}$ has an irregular extension d. We next confine ν to a finite range. By Lemma 2.14, applied to the index system of d (Proposition 2.11), $b > 4000$. Let $\nu_1 = 6$, 8, 6, 7 for $(A, \varepsilon) = (2, 1)$, $(2, -1)$, $(3, 1)$, $(3, -1)$, respectively. For $\nu = \nu_1$ we have $b = 2040$, 1869, 3431, 2584, and for $\nu = \nu_1 + 1$ we have $b = 5335$, 4896, 8968, 6765; since b increases with ν, we get $\nu > \nu_1$. On the other hand $\{a, b, c, d\}$ is a Diophantine quadruple with $a < b < c < d$, $c = a + b + 2\sqrt{ab + 1}$ and $d \ne d_+(a, b, c)$, so $c < 4 \cdot 10^{48}$ by Theorem 7.9. Let $\nu_E = 114$, 116, 113, 115 for the four cases, respectively; at $\nu = \nu_E$ the element c is about $7.39 \cdot 10^{48}$, $6.78 \cdot 10^{48}$, $4.75 \cdot 10^{48}$, $9.37 \cdot 10^{48}$, so $c \ge 4 \cdot 10^{48}$ for every $\nu \ge \nu_E$, as c increases with ν. Hence $\nu_1 < \nu < \nu_E$.

We finally treat the remaining triples, by a finite computation. For each of the 107, 107, 106, 107 triples with $\nu_1 < \nu < \nu_E$, let $M \ge 1$ be an integer just above the zero of Φ_c in $[1, \infty)$, for which $\Phi_c(M) > 0$ was verified. For each $\lambda \in \{-1, 1\}$ a number $J_\lambda \le 3$ satisfying item 1 or item 2 of Proposition B.1 was found, and the exact check of that proposition (no exponent $2m \le J_\lambda$ gives an irregular extension) succeeds. For $\lambda = -1$, the common term $V_1^{-1} = W_1^{-1}$, the number z of the regular extension (Lemma 2.12), makes the number μ_{-1} of Proposition B.1 extremely close to $2 - 2\log\beta/\log\gamma$; in the cases where item 1 was not found, item 2 holds with $(m_0, n_0) = (2, 2)$. All these evaluations were carried out in outward-rounded interval arithmetic with 170 decimal digits. By Proposition B.1, none of these triples has an irregular extension, which contradicts the existence of d. Hence $\{a, b, c\}$ has no irregular extension.

□

8.2 Euler triples of small ratio type

The second family is defined by an arithmetic condition, two elements in a fixed ratio, and it is the application of Theorem 6.3 announced in Section 6. The next lemma describes these triples by a Pell equation, so that those below any bound for c are finite in number and can be listed.

Definition 8.5. Let $j < k$ be coprime positive integers. An Euler triple $\{a, b, c\}$ (Definition 2.3) has **ratio type** $j : k$ if two of its elements $v < w$ satisfy

$$jw = kv.$$

Lemma 8.6. *Let $\{a, b, c\}$ be an Euler triple with root r, of ratio type $j : k$ (Definition 8.5) realised by elements $v < w$ with $jw = kv$, and let $g = \gcd(v, w)$. Then:*

1. *if $(v, w) = (b, c)$ then $k < 4j$, and if $(v, w) = (a, c)$ then $k > 4j$;*
2. *there is a positive integer u with $u^2 - jkg^2 = 1$, and*

$$\begin{aligned}
(v, w) = (a, b): &\quad r = u, \quad c = (j + k)g + 2u;\\
(v, w) = (b, c): &\quad r = u - jg, \quad a = (j + k)g - 2u;\\
(v, w) = (a, c): &\quad r = u - jg, \quad b = (j + k)g - 2u.
\end{aligned}$$

In particular jk is not a square, and every Euler triple of ratio type $j : k$ realised by a given pair of positions arises in this way from a positive solution (u, g) of $u^2 - jkg^2 = 1$, that is, from $u + g\sqrt{jk} = (u_* + g_*\sqrt{jk})^i$ with an integer $i \geq 1$, where (u_*, g_*) is the least positive solution.

Proof. Recall $ab + 1 = r^2$ and $c = a + b + 2r$ (Definition 2.3).

We first prove item 1. By Lemma 2.4, item 4, $a < r < b$ and $c > 4a$; hence $b < c = a + b + 2r < 4b$. If $(v, w) = (b, c)$ then $k/j = c/b < 4$; if $(v, w) = (a, c)$ then $k/j = c/a > 4$.

We next prove item 2. Since $jw = kv$ and $\gcd(j, k) = 1$, j divides v; writing $v = jh$ gives $w = kh$, and $\gcd(v, w) = h \gcd(j, k) = h$, so $v = jg$ and $w = kg$.

If $(v, w) = (a, b)$, then $r^2 = ab+1 = jkg^2+1$, so $u = r$ works and $c = a+b+2r = (j+k)g+2u$.

If $(v, w) = (b, c)$, then $a = c - b - 2r = (k - j)g - 2r$ and

$$r^2 = ab + 1 = jg\big((k - j)g - 2r\big) + 1, \qquad \text{equivalently} \qquad (r + jg)^2 = jkg^2 + 1.$$

Put $u = r + jg \geq 1$. Then $u^2 - jkg^2 = 1$, $r = u - jg$ and $a = (k-j)g-2u+2jg = (j+k)g-2u$.

If $(v, w) = (a, c)$, then $b = c-a-2r = (k-j)g-2r$ and $r^2 = ab+1 = jg\big((k-j)g-2r\big)+1$, which is the same relation as before. Hence $u = r+jg$ satisfies $u^2-jkg^2 = 1$, and $b = (j+k)g-2u$.

We finally prove the last assertion. Since $g \geq 1$ and $u^2 = jkg^2 + 1$, the number jk is not a square: otherwise, with $jk = e^2$, $(u - eg)(u + eg) = 1$ with $u + eg$ a positive integer, which forces $u + eg = 1$ and so $g = 0$. Conversely, the displayed formulas express the triple through (j, k, u, g), so every Euler triple of the given type realised by the given positions arises from a positive solution (u, g) of $u^2 - jkg^2 = 1$. Since jk is not a square, the positive solutions of $u^2 - jkg^2 = 1$ are exactly the pairs with $u + g\sqrt{jk} = (u_* + g_*\sqrt{jk})^i$, $i \geq 1$, where (u_*, g_*) is the least positive solution; this is the classical description of the solutions of Pell's equation (see [15]). □

Theorem 8.7. *Let $\{a, b, c\}$ be an Euler triple of ratio type $j : k$. If $\{a, b, c\}$ has an irregular extension, then*

$$\frac{c}{6(j + k)} - 0.15 < 2.4638 \cdot 10^{12} (\log c)^2 \log \frac{19.46\, c}{6(j + k)}.$$

If $jk \leq 300$, then $\{a, b, c\}$ has no irregular extension.

Proof. We bound m from below linearly in c by the coprime divisors (Theorem 6.3) and compare this bound with the a priori bound (Proposition 7.3); this proves the first assertion and, for $c \geq 10^{21}$, the second, and the triples with $jk \leq 300$ and $c < 10^{21}$, which are finitely many, are treated by a finite computation.

Suppose that $\{a, b, c\}$ has an irregular extension d, and let (λ, l, m, n) be the index system of d (Proposition 2.11). Let $v < w$ be elements realising the ratio type (Definition 8.5), and $g = \gcd(v, w)$, so that $v = jg$ and $w = kg$ because $\gcd(j, k) = 1$.

We first prove $2m > c/(6(j + k))$. By Theorem 6.3, $\Pi_1 \mid m - n$, $\Pi_2 \mid l + \lambda m$, $\Pi_3 \mid l + \lambda n$ and $m > \Pi_1(1 + R_z)$. By Lemma 2.14, $3 \leq n < m < l < 2n$. As $3 \leq n < m$ and $\Pi_1 \mid m - n$, we have $m \geq n + \Pi_1 \geq 3 + \Delta_{ab}$. As $l > m > n$ and $l < 2n < 2m$, we have $1 \leq l + \lambda m \leq l + m < 3m$ and $2 \leq l + \lambda n \leq l + n < 3m$, so the divisibilities $\Pi_2 \mid l + \lambda m$ and $\Pi_3 \mid l + \lambda n$ give $\Pi_2 < 3m$ and $\Pi_3 < 3m$. Since each gcd divisor divides the corresponding coprime divisor (Definition 6.1),

$$m > \max\Big(\Delta_{ab} + 2,\ \tfrac{1}{3}\Delta_{bc},\ \tfrac{1}{3}\Delta_{ac}\Big), \qquad \Delta_{vw} = \frac{\gcd(v, w)}{\gcd(v, w, 4)} \geq \frac{g}{4}.$$

If $(v, w) = (a, b)$, then $c \leq 2(a+b) = 2(j+k)g$ (Lemma 2.4, item 4); hence $m > g/4 \geq c/(8(j+k))$. If $(v, w) \in \{(b, c), (a, c)\}$, then $c = kg$ and $m > g/12 = c/(12k)$. In all cases $2m > c/(6(j + k))$.

We next deduce the first assertion. Put $Y = c/(6(j+k))$, and let Φ_c and K_E be as in Convention 7.1. If $Y \geq 1$, then $\Phi_c(Y) < 0$, since otherwise Proposition 7.3, applied with $u_0 = Y$, would give $2m < Y$; and $\Phi_c(Y) < 0$ is the inequality of the first assertion. Otherwise $\frac{1}{12} < Y < 1$, because $c \geq w = kg \geq k$ and $j < k$; then the left side of the first assertion is less than 1, while its right side is at least $K_E(\log c)^2 \log \frac{19.46}{12} > 1$.

We now prove the second assertion for $c \geq 10^{21}$. Let $jk \leq 300$; since $(j-1)(k-1) \geq 0$, we have $j + k \leq jk + 1 \leq 301$, so $Y \geq c/1806$. We apply Lemma 7.4 with $\iota = 1/1806$, $\theta = 1$ and $c_0 = 10^{21}$. Its hypotheses hold: $\iota c_0 \geq 1$; $\log c_0 > 48.3$ and $|\log(19.46/1806)| < 4.6$; an evaluation in outward-rounded interval arithmetic gives $\Phi_{c_0}(c_0/1806) > 3.0 \cdot 10^{17}$; and $c_0/1806 > 5.5 \cdot 10^{17}$ exceeds $K_E \log c_0\,(2\log(19.46\, c_0/1806) + \log c_0)$, which is less than $1.7 \cdot 10^{16}$. Hence $\Phi_c(c/1806) > 0$ for every $c \geq 10^{21}$, and Proposition 7.3, applied with $u_0 = c/1806 \geq 1$, gives $2m < c/1806 \leq Y$, which contradicts $2m > Y$. So no Euler triple of ratio type $j : k$ with $jk \leq 300$ and $c \geq 10^{21}$ has an irregular extension.

Finally we treat $c < 10^{21}$, by a finite computation. By Lemma 8.6, jk is not a square, and each Euler triple of ratio type $j : k$ arises from a positive solution of $u^2 - jkg^2 = 1$ for one of the three pairs of positions. The triples with $jk \leq 300$ and $c < 10^{21}$ are therefore obtained from finitely many powers of the least positive solutions of these equations; there are 8 906 such triples. For each of them let M be the least integer $M \geq 1$ with $\Phi_c(M) \geq 0$; by Proposition 7.3, an irregular extension would have $2m < M$. For 1 048 of the triples, twice one of the lower bounds for m above, or, when $(v, w) = (a, b)$, twice the lower bound

$$\Delta_{ab}(1 + R_z) = \Delta_{ab} + \frac{\sqrt{ac}}{\gcd(a, b, 4)\,(k - j)} \log \beta \leq \Pi_1(1 + R_z) < m$$

given by Theorem 6.3 (here $b - a = (k - j)g = \gcd(a, b, 4)\Delta_{ab}(k - j)$, and R_z is the gap ratio of Definition 2.16), is at least M; so these triples have no irregular extension. For each of the remaining 7 858 triples and for both signs λ, a number $J_\lambda \leq 11$ satisfying item 1 or item 2 of Proposition B.1 was found, and the exact check of that proposition (no exponent $2m \leq J_\lambda$ gives an irregular extension) succeeds; so these triples have no irregular extension either. Item 1 is the reduction of [16, Lemma 5(a)]. For $\lambda = -1$, the common term $V_1^{-1} = W_1^{-1}$, which is the number z of the regular extension (Lemma 2.12), makes the number μ_{-1} of Proposition B.1 extremely close to $2 - 2\log\beta/\log\gamma$, so that item 1 may fail with denominators q of the size of M; in the cases where item 1 was not found, item 2 holds with $(m_0, n_0) = (2, 2)$. All these evaluations were carried out in outward-rounded interval arithmetic with 150 decimal digits. Hence no Euler triple of ratio type $j : k$ with $jk \leq 300$ has an irregular extension.

□

The first assertion holds for every ratio type. Its left side grows linearly in c and its right side like $(\log c)^3$, so for each $j : k$ it fails for all large c, and by Lemma 8.6 only finitely many triples of ratio type $j : k$ lie below that point: each ratio type is reduced to a finite computation. For $jk \leq 300$ the proof excludes all $c \geq 10^{21}$ in this way, and settles the triples below that bound one by one.

A The three-parameter family for $643 \leq K \leq 2401$

This appendix proves Theorem A.5, which completes Corollary 8.3 in the range $643 \leq K \leq 2401$. It applies the results of Section 5 once more, to the pair representation of the family (Lemma 8.2), now with every quantity bounded in terms of the two parameters $X = F_\nu A$ and K. The quartic floor (Theorem 3.6) and the index inequality Lemma 5.18 become a floor and a ceiling for $2m$

(Lemma A.2), the ceiling being the index function $\mathcal{U}(X,K)$ defined first. Lemma A.3 compares the two, and Lemma A.4 is an exhaustive search over the 1 681 604 parameter points with $F_\nu A \le 144$ and $643 \le K \le 2401$. The plan that combines them is stated at the head of the proof of Theorem A.5.

Definition A.1. With ω as in Convention 5.13 and the exact constants

$$u_1 = 2.47 \cdot 10^{32}, \qquad u_2 = 2.72766\,\sqrt{\omega}, \qquad u_3 = \frac{0.498\,\omega}{60},$$

the **index function** of the three-parameter Fibonacci family (Convention 8.1) is the function of real $X \ge 1$ and $K \ge 643$ given by

$$\mathcal{U}(X,K) = \frac{2\log(u_1 X^7 K)\,\log(u_2 X^{3/2} K)}{\log(4X^2K)\,\log(u_3 K)}.$$

These numerals are the constants of the ceiling for the index in Lemma A.2: u_1 is $1.46\cdot 10^{28}\cdot 10125\big(\frac{5}{3}+\frac{2}{643}\big)$ rounded up, where $1.46\cdot 10^{28}$ is twice the constant $7.3\cdot 10^{27}$ of Lemma 5.18; $u_2/\sqrt{\omega}$ is $0.498\sqrt{30}$ rounded up; and $u_3 = 0.498\,\omega/60$.

Lemma A.2. *Let (ν, A, K, ε) be a parameter point (Convention 8.1) with $\nu A \ge 2$ and $K \ge 643$, and let (λ, l, m, n) be the index system of an irregular extension d of its family triple $\{a,b,c\}$. Then, with the index function $\mathcal{U}$ of Definition A.1,*

1. $2m > (2c)^{1/4} \ge \big(8X^2(K-2)\big)^{1/4}$;
2. $2m < \mathcal{U}(X,K)$.

Proof. Item 1 is Theorem 3.6 with a lower bound for c; item 2 is the index inequality of Lemma 5.18 for the pair representation of the family, with each quantity in it bounded in terms of X and K.

We first fix the pair representation and record elementary bounds. By Lemma 8.2, item 2, $\{a,b,c\}$ is an Euler triple and $(p_1,q_1,p_2,q_2) = (\phi_\nu, \psi_\nu, \phi_{\nu+1}, \psi_{\nu+1})$ is a pair representation of it, with pair coordinates $(p_3,q_3) = (\phi_{\nu+2}, \psi_{\nu+2})$; so $a = f_\nu = p_1q_1$ and $c = f_{\nu+2} = p_3q_3$. Since $\nu \ge 1$,

$$F_\nu \le F_{\nu+1} \le 2F_\nu, \qquad 2F_\nu \le F_{\nu+2} \le 3F_\nu, \qquad F_{\nu+3} \le \min\Big\{5F_\nu,\ 3F_{\nu+1},\ \tfrac{5}{3}F_{\nu+2}\Big\},$$

and $F_k \le \phi_k \le F_{k+1}A$ for $k \ge 0$. Hence

$$X \le \phi_\nu, \qquad \phi_{\nu+1} \le 3X, \qquad 2X + F_{\nu+1} \le \phi_{\nu+2} \le \min\{5X,\ 3\phi_\nu\}, \qquad p_1p_2p_3 \le 30X^3.$$

Moreover $q_3 = \phi_{\nu+2}K + 2\varepsilon F_{\nu+2}$ with $0 < F_{\nu+2} \le \phi_{\nu+2}$ and $AK \ge 643$, so

$$\phi_{\nu+2}(K-2) \le q_3 \le F_{\nu+3}AK + 2F_{\nu+2} \le \Big(\frac{5}{3}+\frac{2}{643}\Big)F_{\nu+2}AK \le 3\Big(\frac{5}{3}+\frac{2}{643}\Big)XK.$$

We now prove item 1. By Theorem 3.6, $c < 8m^4$, that is $2m > (2c)^{1/4}$. By the bounds above, $c = p_3q_3 \ge \phi_{\nu+2}^2(K-2) \ge 4X^2(K-2)$, which gives the second inequality.

We next apply Lemma 5.18. Since $K \geq 643$, Lemma 8.2, item 3, gives $p_1 q_3 \geq \frac{K-2}{3} p_3^2 \geq 213\, p_3^2$; as $p_3 \geq 2X \geq 2$, this gives $p_1 q_3 \geq 852 > 168$ and $\omega p_1 q_3 \geq 213\,\omega p_3^2 > 40\, p_3^2$. Put

$$P = 10\, p_2 p_3 q_3, \qquad L = \frac{\omega p_1 p_2 q_3^2}{4 p_3}, \qquad \Xi = 7.3 \cdot 10^{27}\, p_2^3 p_3^3 q_3, \qquad g = \frac{\log L}{\log(L/P)},$$

so that $L/P = \omega p_1 q_3/(40 p_3^2) > 1$. Then Lemma 5.18 gives $m \log(4ac) < \log 2 + g \log \Xi$. Since $P > 1$ and $L/P > 1$ we have $g > 1$, and $\Xi > 1$; hence

$$m \log(4ac) < g \log 2 + g \log \Xi = g \log(2\Xi).$$

We bound g. With the hypergeometric parameter $N = \frac{1}{2} p_1 p_2 q_3$ and $S_3 = p_1 p_2 p_3$ one has $L = \omega N^2/S_3$ and $L/P = \omega N/(20 p_2 p_3^2)$. For fixed p_1, p_2, p_3, the function

$$N' \mapsto \frac{\log(\omega N'^2/S_3)}{\log\big(\omega N'/(20 p_2 p_3^2)\big)}$$

of real $N' > 0$ is decreasing where its denominator is positive, since there its derivative has the sign of $\log\big(\omega p_1/(400 p_2 p_3^3)\big) < 0$.

Since $q_3 \geq p_3(K-2)$ and $\frac{K}{2} - 1 \geq 0.498K$ (as $K \geq 500$), $N \geq \frac{1}{2} S_3 (K-2) \geq N_0 := 0.498\, S_3 K$. At $N' = N_0$ the denominator is $\log\big(0.498\,\omega p_1 K/(20 p_3)\big) \geq \log(0.498\,\omega K/60) = \log(u_3 K)$, by $p_3 \leq 3p_1$, and $u_3 K \geq 643\, u_3 > 7$. So the denominator is positive on $[N_0, \infty)$, and, as $0.498^2 \omega S_3 K^2 > 1$,

$$g \leq \frac{\log(\omega N_0^2/S_3)}{\log(u_3 K)} = \frac{\log\big(0.498^2\, \omega S_3 K^2\big)}{\log(u_3 K)} \leq \frac{2 \log(u_2 X^{3/2} K)}{\log(u_3 K)},$$

by $S_3 \leq 30 X^3$ and $0.498\sqrt{30} < 2.72766$.

We bound Ξ. By the bounds above, $p_2^3 p_3^3 q_3 \leq (3X)^3 (5X)^3 \cdot 3\big(\frac{5}{3} + \frac{2}{643}\big) XK = 10125\big(\frac{5}{3} + \frac{2}{643}\big) X^7 K$, so

$$2\Xi \leq 1.46 \cdot 10^{28} \cdot 10125 \Big(\frac{5}{3} + \frac{2}{643}\Big) X^7 K < 2.47 \cdot 10^{32} X^7 K = u_1 X^7 K.$$

We bound $4ac$ from below. Write $Y = \phi_\nu \phi_{\nu+2}$. Then $ac = f_\nu f_{\nu+2} = (p_1 q_3)(p_3 q_1)$ with

$$p_1 q_3 = YK + 2\varepsilon \phi_\nu F_{\nu+2}, \qquad p_3 q_1 = YK + 2\varepsilon \phi_{\nu+2} F_\nu.$$

By the bounds above, $Y \geq X(2X + F_{\nu+1})$, $2\phi_\nu F_{\nu+2} \leq 2F_{\nu+1} A \cdot 3F_\nu = 6F_{\nu+1} X$ and $2\phi_{\nu+2} F_\nu \leq 2F_{\nu+3} A F_\nu \leq 6F_{\nu+1} X$. So each factor is at least $2X^2 K + F_{\nu+1} X(K-6) \geq 2X^2 K$, hence $4ac \geq 16 X^4 K^2$, that is $\log(4ac) \geq 2 \log(4X^2 K) > 0$.

We conclude. Combining the three bounds,

$$2m \log(4X^2 K) \leq m \log(4ac) < g \log(2\Xi) \leq \frac{2 \log(u_2 X^{3/2} K)}{\log(u_3 K)} \log(u_1 X^7 K),$$

that is, $2m < \mathcal{U}(X, K)$.

□

Lemma A.3. *Let $\mathcal{U}$ be the index function of the three-parameter family (Definition A.1).*

1. *For every real $X \geq 1$, the function $K \mapsto \mathcal{U}(X, K)$ is positive and decreasing on $[643, \infty)$.*

2. *For all real* $X \geq 145$ *and* $K \geq 643$, $\big(8X^2(K-2)\big)^{1/4} > \mathcal{U}(X,K)$.

3. *For all real* X *and* K *with* $1 \leq X \leq 144$ *and* $K \geq 643$, $\mathcal{U}(X,K) \leq \mathcal{U}(144,643) < 100.6$.

Proof. We first prove item 1. For constants $C_1 > C_2 > 0$, the function $K \mapsto \log(C_1K)/\log(C_2K)$ is positive where $C_2K > 1$, and there its derivative has the sign of $\log(C_2/C_1) < 0$. Write $\mathcal{U} = 2Q_1Q_2$ with

$$Q_1(X,K) = \frac{\log(u_1X^7K)}{\log(4X^2K)}, \qquad Q_2(X,K) = \frac{\log(u_2X^{3/2}K)}{\log(u_3K)}.$$

For $X \geq 1$ and $K \geq 643$ we have $u_1X^7 > 4X^2$, $4X^2K > 1$, $u_2X^{3/2} \geq u_2 > u_3$ and $u_3K \geq 643\,u_3 > 7$. So both factors are positive and decreasing in K on $[643,\infty)$, and so is $\mathcal{U}(X,\cdot)$.

We next prove item 2. For $p > q > 0$ and $C_1, C_2 > 0$, the derivative of the function $X \mapsto \log(C_1X^p)/\log(C_2X^q)$, where $C_2X^q > 1$, has the sign of $\log(C_2^p/C_1^q)$. With $C_1 = 643u_1$, $C_2 = 4 \cdot 643$, $p = 7$, $q = 2$ this sign is that of $\log(4^7 \cdot 643^5/u_1^2) = -107.13\ldots < 0$, so $Q_1(\cdot, 643)$ decreases on $[1,\infty)$. Hence, by item 1, for $X \geq 145$ and $K \geq 643$,

$$\mathcal{U}(X,K) \leq \mathcal{U}(X,643) \leq 2Q_1(145,643)\,Q_2(X,643) =: H(X).$$

Moreover $\big(8X^2(K-2)\big)^{1/4} \geq (8 \cdot 641\,X^2)^{1/4} = 5128^{1/4}X^{1/2} =: L(X)$. Since $Q_2(X,643) = \log(643u_2X^{3/2})/\log(643u_3)$,

$$X\big(L-H\big)'(X) = \tfrac{1}{2}\,5128^{1/4}X^{1/2} - \frac{3\,Q_1(145,643)}{\log(643u_3)},$$

which is increasing in X and positive at $X = 145$ ($50.949\ldots > 10.011\ldots$). So $L - H$ is increasing on $[145,\infty)$, and $L(145) = (8 \cdot 641 \cdot 145^2)^{1/4} = 101.899\ldots > H(145) = \mathcal{U}(145,643) = 100.595\ldots$. Therefore $\big(8X^2(K-2)\big)^{1/4} \geq L(X) > H(X) \geq \mathcal{U}(X,K)$.

We finally prove item 3. By item 1, $\mathcal{U}(X,K) \leq \mathcal{U}(X,643)$, so it suffices to show that $X \mapsto \mathcal{U}(X,643)$ is increasing on $[1,\infty)$. With $w = \log X \geq 0$ and the positive constants $e_1 = \log(643u_1)$, $e_2 = \log 2572$, $e_3 = \log(643u_2)$,

$$\mathcal{U}(X,643) = \frac{2}{\log(643u_3)} \cdot \frac{(e_1+7w)\big(e_3+\frac{3}{2}w\big)}{e_2+2w},$$

and the derivative in w of the last factor has the sign of

$$\Big(7\big(e_3+\tfrac{3}{2}w\big)+\tfrac{3}{2}(e_1+7w)\Big)(e_2+2w)-2(e_1+7w)\big(e_3+\tfrac{3}{2}w\big) = \Big(7e_3+\tfrac{3}{2}e_1\Big)e_2-2e_1e_3+21e_2w+21w^2,$$

which is positive for $w \geq 0$, since its value at $w = 0$ is $139.64\ldots$. Hence $\mathcal{U}(X,K) \leq \mathcal{U}(144,643) = 100.562\ldots < 100.6$ for $1 \leq X \leq 144$ and $K \geq 643$.

All numerical values in this proof were evaluated in interval arithmetic with the exact constants of Definition A.1.

□

The threshold 145 of item 2 is not optimal: its argument already closes from $X = 141$.

Lemma A.4. *Let* (ν, A, K, ε) *be a parameter point (Convention 8.1) with* $\nu A \geq 2$, $F_\nu A \leq 144$ *and* $643 \leq K \leq 2401$. *Then the Pell sequences (Convention 2.6) of its family triple satisfy* $V_m^\lambda = W_n^\lambda$, *with* $\lambda \in \{-1,1\}$ *and integers* $1 \leq m, n \leq 50$, *only for* $(\lambda, m, n) = (-1,1,1)$.

Proof. The proof is a finite computation. There are 478 pairs (ν, A) with $\nu A \geq 2$ and $F_\nu A \leq 144$, all with $\nu \leq 12$, hence $478 \cdot 1759 \cdot 2 = 1\,681\,604$ parameter points as in the statement. At each of them the family triple $\{a, b, c\}$ is an Euler triple with root r (Lemma 8.2, item 2), and its other roots are $s = a + r$ and $t = b + r$. At each point, a, b, c, r were computed in exact integer arithmetic and the identities of Lemma 8.2, item 1, were checked; then V_j^λ and W_j^λ were computed for both λ and $0 \leq j \leq 50$ by the recurrences and initial terms of item 3 of Lemma 2.8, modulo the prime $2^{31} - 1$. A non-congruence $V_m^\lambda \not\equiv W_n^\lambda$ modulo $2^{31} - 1$ proves $V_m^\lambda \neq W_n^\lambda$. Besides $(\lambda, m, n) = (-1, 1, 1)$, which gives a congruence at every point, there are fifteen congruences with $1 \leq m, n \leq 50$, at four parameter points; each of them was recomputed in exact integer arithmetic, and none is an equality. This proves the claim.

The exception is a genuine common term: by Lemma 2.12, $V_1^{-1} = W_1^{-1}$ is the number z of the regular extension $d_+(a, b, c)$.

□

Theorem A.5. *Let (ν, A, K, ε) be a parameter point (Convention 8.1) with $\nu A \geq 2$ and $643 \leq K \leq 2401$. Then its family triple has no irregular extension.*

Proof. The floor and the ceiling for the index (Lemma A.2) are incompatible when $X \geq 145$; when $X \leq 144$ the ceiling leaves only indices $m \leq 50$, which the search of Lemma A.4 excludes.

By Lemma 8.2, item 2, the family triple $\{a, b, c\}$ is an Euler triple. Suppose that it has an irregular extension d, and let (λ, l, m, n) be the index system of d (Proposition 2.11). By Lemma A.2,

$$\big(8X^2(K-2)\big)^{1/4} < 2m < \mathcal{U}(X, K).$$

Since X is a positive integer, either $X \geq 145$ or $X \leq 144$. If $X \geq 145$, this contradicts Lemma A.3, item 2.

Let $X \leq 144$. By Lemma A.3, item 3, $2m < \mathcal{U}(X, K) < 100.6$, so $m \leq 50$; and Lemma 2.14 gives $3 \leq n < m$. By item 2 of Lemma 2.8, $V_m^\lambda = z = W_n^\lambda$ with $3 \leq n < m \leq 50$. This contradicts Lemma A.4, since $m \neq 1$.

Hence $\{a, b, c\}$ has no irregular extension. □

B A Baker–Davenport reduction for a single Euler triple

For a single Euler triple the a priori bound leaves finitely many indices: $2m < M$ for every integer M with $\Phi_c(M) \geq 0$ (Proposition 7.3). By the method of Baker and Davenport [4], in the inhomogeneous form of Dujella and Pethő [16], the linear form Λ_z, divided by $\log \gamma$, reduces them to $2m \leq J_\lambda$ for a small J_λ, and these are checked directly; Proposition B.1 states the resulting criterion. Its second alternative serves the sign $\lambda = -1$, for which the common term $V_1^{-1} = W_1^{-1}$ of the regular extension can make the number μ_{-1} extremely close to $2 - 2\log\beta/\log\gamma$, so that the first alternative does not apply with denominators of the size of M. The criterion is used in Theorem 8.4 and Theorem 8.7.

Proposition B.1. *Let $\{a, b, c\}$ be an Euler triple with units β, γ and multiplication matrix $\mathbf{B}$ (Definition 2.3), and let $M \geq 1$ be an integer with $\Phi_c(M) \geq 0$, where Φ_c is as in Convention 7.1. For $\lambda \in \{-1, 1\}$ let E_λ and κ_λ be as in Definition 2.16, and put*

$$\xi = \frac{\log \beta}{\log \gamma}, \qquad \mu_\lambda = \frac{\log E_\lambda}{\log \gamma}.$$

Suppose that for each $\lambda \in \{-1, 1\}$ there is an integer $J_\lambda \geq 0$ for which one of the following holds.

1. *There are integers p, q with $q > 0$ such that $\eta = \|q\mu_\lambda\| - M|q\xi - p| > 0$, where $\|\cdot\|$ denotes the distance to the nearest integer, and $q\kappa_\lambda \le \eta\,\beta^{2J_\lambda}\log\gamma$.*

2. *There are integers $m_0 \ge 0$ and n_0 with $m_0 < J_\lambda$ such that*

$$|m_0\xi - n_0 + \mu_\lambda| + \frac{\kappa_\lambda}{\log\gamma}\,\beta^{-2J_\lambda} < \min\{|q\xi - p| :\ p/q \text{ a convergent of } \xi,\ 1 \le q < M\}.$$

If, for each λ and each integer $m \ge 0$ with $2m \le J_\lambda$, the second coordinate x of $\mathbf{B}^{2m}\binom{\lambda}{1}$ does not give an integer $d = (x^2-1)/a$ with $d > c$, $d \ne d_+(a,b,c)$ and $bd+1$ a square, then $\{a,b,c\}$ has no irregular extension.

Proof. Suppose that d is an irregular extension of $\{a,b,c\}$, let (λ, l, m, n) be the index system of d (Proposition 2.11), and let x, y, z be as in Definition 2.5. By item 2 of Lemma 2.8, $\binom{z}{x} = \mathbf{B}^{2m}\binom{\lambda}{1}$; so x is the second coordinate of $\mathbf{B}^{2m}\binom{\lambda}{1}$. By Proposition 7.3, applied with $u_0 = M$, we have $2m < M$.

We show that $2m \le J_\lambda$. Suppose $2m > J_\lambda$. Item 5 of Lemma 2.18, divided by $\log\gamma$, gives

$$0 < 2m\xi - 2n + \mu_\lambda < \frac{\kappa_\lambda}{\log\gamma}\,\beta^{-4m} < \frac{\kappa_\lambda}{\log\gamma}\,\beta^{-2J_\lambda}.$$

In case 1 we use the reduction of Baker and Davenport [4], in the inhomogeneous form of [16, Lemma 5(a)]. Since $q\mu_\lambda - q(2m\xi - 2n + \mu_\lambda) + 2m(q\xi - p)$ is an integer and $2m < M$,

$$\|q\mu_\lambda\| \le q\,(2m\xi - 2n + \mu_\lambda) + 2m|q\xi - p| < \frac{q\kappa_\lambda}{\log\gamma}\,\beta^{-4m} + M|q\xi - p|,$$

so $q\kappa_\lambda\beta^{-4m} > \eta\log\gamma$, that is $\eta\,\beta^{4m}\log\gamma < q\kappa_\lambda \le \eta\,\beta^{2J_\lambda}\log\gamma$, which contradicts $2m > J_\lambda$. In case 2, $2m - m_0 \ge 1$ and

$$|(2m - m_0)\xi - (2n - n_0)| \le |2m\xi - 2n + \mu_\lambda| + |m_0\xi - n_0 + \mu_\lambda| < \frac{\kappa_\lambda}{\log\gamma}\,\beta^{-2J_\lambda} + |m_0\xi - n_0 + \mu_\lambda|.$$

The number ξ is irrational: $\beta^Q = \gamma^P$ with integers $P, Q \ge 1$ is impossible, since $\beta^Q \in \mathbb{Q}(\sqrt{ac})\setminus\mathbb{Q}$ and $\gamma^P \in \mathbb{Q}(\sqrt{bc})$, and these two fields are distinct because ab is not a square (Lemma 2.4, item 5). Let p_i/q_i be the convergent of ξ with $q_i \le 2m - m_0 < q_{i+1}$. By the best-approximation property of convergents, $|(2m - m_0)\xi - (2n - n_0)| \ge |q_i\xi - p_i|$, and $1 \le q_i \le 2m - m_0 < M$; this contradicts the hypothesis of case 2.

Hence $2m \le J_\lambda$, and $d = (x^2-1)/a$ with x the second coordinate of $\mathbf{B}^{2m}\binom{\lambda}{1}$, $d > c$, $d \ne d_+(a,b,c)$ (as d is irregular, Definition 2.2) and $bd+1 = y^2$. This contradicts the hypothesis. □

Acknowledgements

This paper was prepared with the assistance of Aleph, an AI research assistant for mathematics, using an ensemble of AI models from Anthropic (Claude), OpenAI (ChatGPT) and Google (Gemini) together with bespoke AI models. The authors take full responsibility for the content of the paper and for all mathematical results.

References

[1] K. Adédji, M. Trebješanin, A. Filipin et al., *On the $D(4)$-pairs $\{a, ka\}$ with $k \in \{2,3,6\}$*, Glas. Mat., III. Ser. **58** (2023), 35-57.

[2] K. N. Adédji, A. Filipin and A. Togbé, *On the family of Diophantine pairs* $\{P_{2k}, 2P_{2k+2}\}$, Fibonacci Quart. **60** (2022), no. 1.

[3] J. Arkin, V. E. Hoggatt and E. G. Straus, On Euler's solution of a problem of Diophantus, Fibonacci Quart. 17 (1979), 333–339.

[4] A. Baker and H. Davenport, The equations 3xˆ2-2=yˆ2 and 8xˆ2-7=zˆ2, Q. J. Math. Oxford Ser. (2) 20 (1969), 129–137.

[5] M. Bennett, *Simultaneous rational approximation to binomial functions*, Trans. Am. Math. Soc. **348** (1996), 1717-1738.

[6] M. A. Bennett, On the number of solutions of simultaneous Pell equations, J. Reine Angew. Math. 498 (1998), 173–199.

[7] M. Cipu, Y. Fujita and M. Mignotte, Two-parameter families of uniquely extendable Diophantine triples, Sci. China Math. 61 (2018), 421–438.

[8] M. Cipu, A. Filipin and Y. Fujita, Bounds for Diophantine Quintuples II, Publicationes Mathematicae Debrecen 88 (2016), 59–78.

[9] M. Cipu and Y. Fujita, Bounds for Diophantine quintuples, Glas. Mat. Ser. III 50(70) (2015), 25–34.

[10] M. Cipu, Y. Fujita, and M. Mignotte, *Diophantine triples with three parameters*, Res. Number Theory **10** (2024), Paper No. 44, 23 p..

[11] M. Cipu, Y. Fujita and T. Miyazaki, On the Number of Extensions of a Diophantine Triple, International Journal of Number Theory 14 (2018), 899–917.

[12] A. Dujella, A proof of the Hoggatt-Bergum conjecture, Proc. Amer. Math. Soc. 127 (1999), 1999–2005.

[13] A. Dujella, An absolute bound for the size of Diophantine m-tuples, J. Number Theory 89 (2001), 126–150.

[14] A. Dujella, There are only finitely many Diophantine quintuples, J. Reine Angew. Math. 566 (2004), 183–214.

[15] A. Dujella, Diophantine m-tuples and Elliptic Curves, Developments in Mathematics 79, Springer, Cham, 2024.

[16] A. Dujella and A. Pethő, A generalization of a theorem of Baker and Davenport, Q. J. Math. Oxford Ser. (2) 49 (1998), 291–306.

[17] A. Filipin, Y. Fujita and A. Togbé, The extendibility of Diophantine pairs. II: Examples, Journal of Number Theory 145 (2014), 604–631.

[18] Y. Fujita and T. Miyazaki, The regularity of Diophantine quadruples, Transactions of the American Mathematical Society 370 (2018), 3803–3831.

[19] B. He, A. Togbé and V. Ziegler, There is no Diophantine quintuple, Trans. Amer. Math. Soc. 371 (2019), 6665–6709.

[20] B. He and A. Togbé, There are only finitely many irregular Diophantine quadruples, preprint, arXiv:2610.18912, 2026.

[21] B. W. Jones, A second variation on a problem of Diophantus and Davenport, Fibonacci Quart. 16 (1978), 155–165.

[22] M. Laurent, Linear forms in two logarithms and interpolation determinants II, Acta Arith. 133 (2008), 325–348.

[23] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II, Izvestiya: Mathematics 64 (2000), 1217–1269.

[24] M. Mignotte and P. Voutier, A kit for linear forms in three logarithms, with an appendix by M. Laurent, Math. Comp. 93 (2024), 1903–1951.

[25] J. Park and J. Lee, *Some family of Diophantine pairs with Fibonacci numbers*, Indian J. Pure Appl. Math. **50** (2019), 367-384.

[26] J. H. Rickert, Simultaneous rational approximation and related Diophantine equations, Math. Proc. Cambridge Philos. Soc. 113 (1993), 461–472.

(A. Dujella) Department of Mathematics, University of Zagreb, Croatia
E-mail address: duje@math.hr

(S. Slijepčević) Department of Mathematics, University of Zagreb, Croatia
Cantab Pi, Cambridge, UK
E-mail address: sinisa@math.hr, sinisa@cantabpi.com