

Rational Fourth Powers Summing to 82

A complete solution to the generalised Fermat equation

$$x^4 + y^4 = 82z^4$$

Natanael Wildner Fraga

15 October 2026

Abstract

We prove that the only primitive positive integer solutions of $x^4 + y^4 = 82z^4$ are $(1, 3, 1)$ and $(3, 1, 1)$. An arithmetic reduction lifts every other putative solution to an elliptic curve over $K = \mathbb{Q}(\sqrt{41}, \sqrt{2})$. An explicit 2-descent determines its rank as 3. A logarithmic functional then excludes all nonzero parameters in the relevant 2-adic disc, including both relative sign patterns at the two places above 2. The same argument determines every point of the auxiliary quartic whose parameter is rational: only the two points at infinity occur. Exact square identities also determine the quotient modulo 2, prove that the displayed subgroup has odd index, and give the vanishing of the 2-primary part of the Tate–Shafarevich group. Two reductions determine the torsion. The finite arithmetic certificates are supplied in two self-contained Python programs; no height cutoff or conjectural rank computation is used.

Keywords: generalised Fermat equation; rational fourth powers; elliptic Chabauty; 2-descent; biquadratic fields.

1 The problem and the main theorem

The identity $1^4 + 3^4 = 82$ gives a solution. The problem is to prove completeness. Ratcliffe and Grechuk (2025, Section 2.1) list the coefficient 82 as the remaining open case of the family $x^4 + y^4 = cz^4$ with $1 \leq c \leq 100$. The covering approach has a precedent in the treatment of the coefficient 17 by Flynn and Wetherell (2001).

A nonzero integer triple is *primitive* if its coordinates have greatest common divisor 1.

Theorem 1.1. *Every integer solution of*

$$x^4 + y^4 = 82z^4 \tag{1.1}$$

satisfies

$$\{|x|, |y|\} = \{|z|, 3|z|\}. \tag{1.2}$$

Consequently, the only primitive positive solutions are $(1, 3, 1)$ and $(3, 1, 1)$. All integer solutions follow by independent signs, interchange of the first two coordinates, and common integer scaling, including the zero solution.

Sections 2–3 give the arithmetic reduction and the covering. Sections 4–6 establish the descent and the rank. Sections 7–8 determine the rational parameters and complete the proof. Section 9 records the additional group-theoretic conclusions. Section 10 and the appendices specify the finite certificates.

2 Arithmetic reduction

Take a primitive nonzero solution. Its coordinates are pairwise coprime: a prime dividing x and y but not z would have its fourth power divide 82; the other two pairs follow directly from (1.1). Reduction modulo 16 shows that x, y, z are odd.

Modulo 41, the quotient x/y is one of $\pm 3, \pm 14$. Changing one sign permits the assumption

$$41 \mid (3x - y)(x - 3y).$$

Put

$$\begin{aligned} S_0 &= x^2 + y^2, & P_0 &= xy, \\ q &= 5S_0 - 3P_0, & r_0 &= (3S_0 - 10P_0)/2. \end{aligned}$$

Here $q > 0$ is odd and r_0 is even. Direct expansion gives

$$q^2 - 2r_0^2 = \frac{41}{2}(x^4 + y^4) = 41^2 z^4. \quad (2.1)$$

Since $2r_0 = (3x - y)(x - 3y)$, both r_0 and q are divisible by 41. Write

$$A = q/41, \quad B_0 = r_0/41 = 2L.$$

The inverse identities

$$S_0 = 10A - 6B_0, \quad P_0 = 3A - 10B_0$$

and $\gcd(S_0, P_0) = 1$ give $\gcd(A, B_0) = 1$, hence $\gcd(A, z) = 1$. Set $u = (x + y)/2$ and $v = (x - y)/2$. Then

$$\begin{aligned} u^2 &= 4A - 13L, \\ v^2 &= A + 7L, \\ A^2 - 8L^2 &= z^4. \end{aligned} \quad (2.2)$$

The nonnegative integers $(A + z^2)/2$ and $(A - z^2)/2$ are coprime, have opposite parity, and have product $2L^2$. In some order they are m^2 and $2n^2$, where $m > 0$ is odd, $\gcd(m, n) = 1$, and the sign of n is chosen so that $L = mn$. Thus

$$A = m^2 + 2n^2, \quad z^2 = \pm(m^2 - 2n^2).$$

The negative sign is impossible modulo 3. If exactly one of m, n is divisible by 3, then $2n^2 - m^2$ is 2 modulo 3. If neither is divisible by 3, the first two right sides of (2.2) become $-mn$ and mn modulo 3, and one is 2. Both cannot be divisible by 3. We have therefore obtained

$$\begin{aligned} u^2 &= 4m^2 - 13mn + 8n^2, \\ v^2 &= m^2 + 7mn + 2n^2, \\ z^2 &= m^2 - 2n^2, \end{aligned} \quad (2.3)$$

with $m > 0$ odd and $\gcd(m, n) = 1$. If $n = 0$, then $m = 1$ and the asserted solutions follow. It remains to exclude $n \neq 0$.

Lemma 2.1. *Every solution of (2.3) satisfies $32 \mid n$.*

Proof. The third equation modulo 8 forces $2 \mid n$. Write $n = 2k$. The first equation modulo 4 forces $2 \mid k$, and the second equation modulo 8 then forces $8 \mid n$. With $n = 8j$, divide the first equation by 4:

$$(u/2)^2 = m^2 - 26mj + 128j^2.$$

The right side is odd. Modulo 8 it follows that $2mj$ is divisible by 8. Since m is odd, $4 \mid j$. $\square$

3 The elliptic covering

Throughout the remaining sections, put

$$\begin{aligned} r &= \sqrt{41}, & s &= \sqrt{2}, \\ \alpha &= (1 + r)/2, & K &= \mathbb{Q}(r, s), \\ \alpha^2 &= \alpha + 10. \end{aligned}$$

Define

$$\begin{aligned} a_+ &= (13 + r)/8, \\ a_- &= (13 - r)/8, \\ b &= (-7 + r)/2 = \alpha - 4, \\ b_- &= (-7 - r)/2. \end{aligned} \tag{3.1}$$

Lemma 3.1. *For a solution of (2.3), all six elements*

$$\begin{aligned} m - a_+n, & \quad m - a_-n, \\ m - bn, & \quad m - b_-n, \\ m - sn, & \quad m + sn \end{aligned}$$

are squares in K .

Proof. The field $\mathbb{Q}(r)$ has class number 1. Its Minkowski bound is $\sqrt{41}/2 < 3.21$; the prime 3 is inert and the primes of norm 2 are principal, generated by $(7 \pm r)/2$. The unit $32 + 5r$ has norm -1 . Therefore every totally positive unit of this real quadratic field is a square.

The first four elements are algebraic integers because $32 \mid n$. They are units at both places above 2 because m is odd. Their norms are respectively $u^2/4, u^2/4, v^2, v^2$.

There are no factors above 41. Indeed, if $41 \mid u$, the identity

$$(8m - 13n)^2 - 41n^2 = 16u^2$$

would have valuation exactly 1 on the left: coprimality makes n a unit at 41, and $8m - 13n$ is divisible by 41. The identity

$$(2m + 7n)^2 - 41n^2 = 4v^2$$

treats v in the same way. Away from 2 and 41, conjugate factors are coprime. An inert prime cannot occur, since it would divide both factors; at a split prime the square norm forces an even valuation. Thus each of the four principal ideals is a square.

For $n \neq 0$, the three real square conditions in (2.3) imply

$$T = m/n \geq a_+ \quad \text{or} \quad T \leq b_-.$$

Since $m > 0$, all four homogeneous factors are totally positive in either case. Class number 1 and the unit assertion make them squares in $\mathbb{Q}(r)$. The case $n = 0$ has $m = 1$.

For the last two factors, work in $\mathbb{Q}(s)$. Its Minkowski bound is $\sqrt{8}/2 < 2$, its class number is 1, and $1 + s$ has norm -1 . The two factors are coprime, including above 2, and have product z^2 . They are totally positive because $m > |sn|$. The same argument applies. $\square$

Let G be the affine quartic

$$G : \quad V^2 = (T - a_+)(T - a_-) \cdot (T - b)(T - s). \quad (3.2)$$

If $n \neq 0$, Lemma 3.1 shows that $T = m/n$ is the parameter of a point of $G(K)$: divide the product of the four corresponding homogeneous squares by n^4 .

We will prove a stronger statement. The quartic is monic with four distinct roots. Let $\overline{G}$ be the smooth projective model and let $\pi : \overline{G} \rightarrow \mathbb{P}^1$ be the function T . Its two points above infinity, denoted ∞_+ and ∞_- , are characterized by $V/T^2 = 1$ and -1 .

Theorem 3.2. *The only points of $\overline{G}(K)$ with parameter in $\mathbb{P}^1(\mathbb{Q})$ are ∞_+ and ∞_- . Equivalently, for no finite $T \in \mathbb{Q}$ is the right side of (3.2) a square in K .*

This concerns rational parameters, not all points of $\overline{G}(K)$. Its proof is completed in Section 8.

For field elements use the coordinates

$$[c_0, c_1, c_2, c_3] = c_0 + c_1\alpha + c_2s + c_3\alpha s.$$

Set

$$\begin{aligned} D &= [-68, 13, 45, -8], \\ B &= D^2(-4 - 3s) \\ &= [2624, -656, -2132, 533], \\ e_2 &= D(1 + s) = [22, -3, -23, 5], \\ e_3 &= D(-2 - s). \end{aligned}$$

The elliptic curve is

$$\begin{aligned} E : \quad Y^2 &= X^3 + DX^2 + BX \\ &= X(X - e_2)(X - e_3). \end{aligned} \quad (3.3)$$

Put

$$\begin{aligned} X_P &= [164, -41, 0, 0], \\ Y_P &= [-2132, 574, -328, 82] \\ &= 2(b - s)X_P. \end{aligned}$$

Then $P = (X_P, Y_P)$ lies on E . The birational transformation is

$$\begin{aligned} X &= X_P \frac{T - s}{T - b}, \\ Y &= Y_P \frac{V}{(T - b)^2}, \\ T &= \frac{bX - sX_P}{X - X_P}. \end{aligned} \quad (3.4)$$

Substitution verifies the polynomial identity. The two points at infinity on G map to P and $-P$.

4 Field arithmetic and square classes

The discriminants of the two generating quadratic fields are coprime. Hence

$$\begin{aligned} \mathcal{O}_K &= \mathbb{Z}[\alpha, s], \\ \text{disc}(K) &= 8 \cdot 41 \cdot 328 = 107584. \end{aligned}$$

The Minkowski bound is

$$\frac{4!}{4^4} \sqrt{107584} = 30.75.$$

The only prime ideals of norm at most this bound lie above 2, 3, 5, and 23, with norms 2, 9, 25, and 23 respectively.

Consider the units

$$\begin{aligned} -1, \quad \varepsilon_2 &= 1 + s, \\ \varepsilon_{41} &= 27 + 10\alpha, \quad \eta = [11, 4, 8, 3]. \end{aligned}$$

Their norms are 1, 1, 1, -1 , and

$$\eta^2 = (1 + s)(32 + 5r)(9 + rs).$$

Order the four real embeddings by the signs of (r, s) as $(+, +), (+, -), (-, +), (-, -)$. Encode a negative sign at the embedding of index j by the bit 2^j , with indices starting at zero. The four unit masks are

$$15, \quad 10, \quad 12, \quad 2.$$

They are independent over $\mathbb{F}_2$. The unit theorem gives dimension 4 for units modulo squares, so these units form a basis. In particular, every totally positive unit of K is a square.

Put

$$\begin{aligned} \pi_0 &= 3 + \alpha, \quad \gamma = 13 + 8s, \\ h &= [1, 1, 2, 1]. \end{aligned}$$

Then $h^2 = \pi_0 \gamma$ and $N_{K/\mathbb{Q}}(h) = -82$. Let $\mathcal{P}$ be the prime above 2 with $\mathcal{P}^2 = (\pi_0)$. This prime is not principal. Otherwise total positivity of π_0 and the unit calculation would make π_0 a square in K . Since $\pi_0 \in \mathbb{Q}(r)$, either π_0 or $\pi_0/2$ would then be a square in $\mathbb{Q}(r)$. Their norms are 2 and $1/2$, neither a rational square.

The following norm certificates determine the remaining classes needed for Minkowski's bound.

Element	Norm
$[-20, -5, -9, -5]$	-46
$[-19, -7, -8, -3]$	-18
$[-19, 4, -13, 3]$	-25

The first two principal ideals are products of a prime above 2 and a prime of norm 23 or 9. The third is a prime of norm 25. The two primes above 2 have the same class: their product is (s) and each class has order dividing 2. Conjugation treats all primes above 3, 5, and 23. Thus

$$\text{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}. \quad (4.1)$$

Let S be the four primes above 2 and 41. The ring of S -integers has trivial class group. A basis of its units modulo squares, in the order used below, is

$$\begin{aligned} &(g_0, \dots, g_7) \\ &= (-1, \varepsilon_2, \varepsilon_{41}, \eta, \pi_0, s, r, h). \end{aligned} \quad (4.2)$$

To check completeness, order S as $\mathcal{P}, \mathcal{P}', \mathcal{Q}, \mathcal{Q}'$, where $(\gamma) = \mathcal{Q}^2$ and $(h) = \mathcal{P}\mathcal{Q}$. The valuation vectors of the last four generators are

$$\begin{aligned} (2, 0, 0, 0), \quad (1, 1, 0, 0), \\ (0, 0, 1, 1), \quad (1, 0, 1, 0). \end{aligned}$$

Their determinant has absolute value 2, precisely the index of principal ideals in the lattice of ideals supported in S . The first four generators already give every ordinary unit class. This proves (4.2).

5 The 2-descent

5.1 The global Kummer map

The injective Kummer map is

$$\begin{aligned}\mu : E(K)/2E(K) &\longrightarrow (K^*/K^{*2})^2, \\ \mu(X, Y) &= (X, X - e_2).\end{aligned}\tag{5.1}$$

Writing $T_0 = (0, 0)$ and $T_2 = (e_2, 0)$, its exceptional values are

$$\begin{aligned}\mu(T_0) &= (e_2 e_3, -e_2), \\ \mu(T_2) &= (e_2, e_2(e_2 - e_3)), \\ \mu(O) &= (1, 1).\end{aligned}$$

The omitted third component is the product of the first two. The line-intersection law makes this map a homomorphism; the halving formula obtained from square roots of $X, X - e_2, X - e_3$ identifies its kernel with $2E(K)$.

The nonzero roots and all root differences are units outside S ; in particular,

$$N_{K/\mathbb{Q}}(D) = -2 \cdot 41^3.$$

Outside S every component of a Kummer image has even valuation. Since the ring of S -integers has trivial class group, each component has a representative in (4.2). There are $2^{16} = 65536$ pairs to test.

5.2 Local square classes

At either place above 2 the completion is $\mathbb{Q}_2(s)$. The place is specified by $\alpha \equiv 0$ or 1 modulo 2. Use the four-bit square-class basis

$$(s, -1, 1 + s, 1 + 2s).$$

The first bit records valuation parity. For a unit $a + bs$, the exact square criterion is

$$(a \bmod 8, b \bmod 4) = (1, 0) \quad \text{or} \quad (3, 2).\tag{5.2}$$

Necessity follows by squaring a unit. Sufficiency follows from Hensel's lemma, since the congruence is modulo s^5 and $5 > 2v_s(2) = 4$.

At either place above 41 the completion is $\mathbb{Q}_{41}(r)$, with $s \equiv 17$ or 24 modulo 41. Use the two-bit basis $(r, 3)$; the unit 3 is nonsquare modulo 41. If the two component codes are c_1, c_2 , their pair code is $c_1 + 2^d c_2$, where $d = 4$ above 2 and $d = 2$ above 41.

The following two tables give the images of (4.2) and bases of the local Kummer images. Congruences in the place labels are taken modulo the indicated rational prime.

Place	Generator codes, in order
2, $\alpha \equiv 0$	2, 4, 2, 0, 10, 1, 8, 8
2, $\alpha \equiv 1$	2, 4, 0, 4, 10, 1, 10, 1
41, $s \equiv 17$	0, 0, 0, 0, 2, 2, 1, 2
41, $s \equiv 24$	0, 0, 0, 0, 2, 2, 1, 1

Place	Basis of the local image
2, $\alpha \equiv 0$	179, 73, 17, 6
2, $\alpha \equiv 1$	35, 64, 169, 41
41, $s \equiv 17$	2, 10
41, $s \equiv 24$	14, 3

These are complete local images, not merely subspaces supplied by selected points. At a place above 2,

$$\dim_{\mathbb{F}_2} E(K_v)/2E(K_v) = [K_v : \mathbb{Q}_2] + \dim_{\mathbb{F}_2} E(K_v)[2] = 4.$$

At a place above 41 the dimension is 2. The displayed bases attain these dimensions. In addition to T_0, T_2 , suitable witnesses have X coordinates $4s, 1 + 3s$ at the first place, $6s, 12s$ at the second, and 3 at the third. At the third place use the isomorphic local model with D replaced by $D/41$; the scaling factor $41 = r^2$ is a local square. The product of the three cubic factors is a square for each witness. The verifier reconstructs and tests these classes.

At the four real embeddings ordered as in Section 4, the masks of negative signs among the eight generators are 1, 171, 197, 231. The allowed pair codes are respectively

$$\{0, 3\}, \quad \{0, 2\}, \quad \{0, 1\}, \quad \{0, 2\}.$$

These follow from the two intervals on which the real cubic is nonnegative.

5.3 The finite upper bound

Encode a global square class by an eight-bit mask in (4.2), and a pair by $A_0 + 256B_0$. Intersecting the four finite local conditions and the four real conditions gives the five-dimensional space $\mathcal{C}$ with basis

$$14, \quad 672, \quad 1425, \quad 2048, \quad 41249. \quad (5.3)$$

Direct enumeration gives exactly 32 elements. Equivalently, the binary restrictions have rank 11 in 16 variables. Since E has full rational 2-torsion,

$$\begin{aligned} \text{rank } E(K) + 2 &= \dim_{\mathbb{F}_2} E(K)/2E(K) \leq 5, \\ \text{rank } E(K) &\leq 3. \end{aligned} \quad (5.4)$$

This upper bound uses only necessary local conditions. It does not require every class in $\mathcal{C}$ to be globally soluble.

6 Points, rank, and the quotient modulo 2

Besides P , use $Q = (X_Q, Y_Q)$ and $R = (X_R, Y_R)$ with

$$\begin{aligned} 36X_Q &= 1100827 - 297329\alpha \\ &\quad - 777800s + 210120\alpha s, \\ 216Y_Q &= 2144893701 \\ &\quad - 579455603\alpha - 1516659202s \\ &\quad + 409733998\alpha s, \\ 392X_R &= 70882 - 16673\alpha \\ &\quad - 48356s + 12854\alpha s, \\ 10976Y_R &= 38328084 - 10524898\alpha \\ &\quad - 27190638s + 7268179\alpha s. \end{aligned} \quad (6.1)$$

Exact substitution verifies all three points on (3.3).

Proposition 6.1. *The images of T_0, T_2, P, Q, R form a basis of $E(K)/2E(K)$. Their pair codes, in that order, are*

$$41249, \quad 672, \quad 42512, \quad 2048, \quad 14. \quad (6.2)$$

Consequently, $E(K)$ has rank 3 and the subgroup

$$H = \langle T_0, T_2, P, Q, R \rangle$$

has finite odd index in $E(K)$.

Proof. Appendix A supplies ten exact square identities giving the two Kummer components of each point. The five codes in (6.2) are independent and span the space in (5.3). In particular,

$$42512 \oplus 41249 \oplus 672 = 1425,$$

where $\oplus$ denotes bitwise addition modulo 2. Thus the upper bound (5.4) is attained. Moreover, $H + 2E(K) = E(K)$. The finitely generated quotient $E(K)/H$ has surjective multiplication by 2, so it is finite of odd order. $\square$

The proposition does not assert that this odd index is 1. The logarithmic argument below requires only a subgroup of full rank.

7 The logarithmic certificate

Write

$$\mathcal{K} = K \otimes_{\mathbb{Q}} \mathbb{Q}_2, \quad \mathcal{R} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_2.$$

Let Log be the elliptic logarithm normalized by $dX/(2Y)$, extended from the formal group by division after multiplication into that group. It is defined componentwise on $E(\mathcal{K})$ and vanishes on torsion. All coordinates in this section use $(1, \alpha, s, \alpha s)$.

7.1 A finite logarithm computation

Let M be the matrix with rows

$$\frac{\text{Log}(16P)}{32}, \quad \frac{\text{Log}(16Q)}{32}, \quad \frac{\text{Log}(16R)}{16}.$$

It is integral and satisfies

$$M \equiv \begin{pmatrix} 427 & 100 & 180 & 352 \\ 185 & 477 & 78 & 70 \\ 385 & 461 & 290 & 468 \end{pmatrix} \pmod{512}. \quad (7.1)$$

Here is a direct certificate. Represent K using

$$\theta = r + s, \quad \theta^4 - 86\theta^2 + 1521 = 0.$$

Four doublings, using

$$X(2Z) = \frac{(X(Z)^2 - B)^2}{4Y(Z)^2},$$

put the formal parameter $\tau = -X(16Z)/Y(16Z)$ in $16\mathcal{R}$ for $Z = P, Q, R$. In this parameter the invariant differential is

$$\frac{d\tau}{\sqrt{1 - 2D\tau^2 + (D^2 - 4B)\tau^4}}.$$

The coefficient of τ^{2j} is the algebraic integer

$$c_j = \sum_{0 \leq 2i \leq j} \binom{j}{2i} \binom{2i}{i} D^{j-2i} B^i.$$

Thus the logarithm has coefficient $c_j/(2j+1)$ in degree $2j+1$. All denominators are odd. Since $\tau \in 16\mathcal{R}$, it follows that

$$\text{Log}(\tau) \equiv \tau + \frac{D}{3}\tau^3 \pmod{2^{16}\mathcal{R}}; \quad (7.2)$$

the omitted terms are in $2^{20}\mathcal{R}$. Exact arithmetic gives the following coordinates modulo 65536:

$$\begin{aligned} \text{Log}(16P) &\equiv [13664, 35968, 5760, 60416], \\ \text{Log}(16Q) &\equiv [38688, 64416, 2496, 35008], \\ \text{Log}(16R) &\equiv [63504, 7376, 4640, 23872]. \end{aligned}$$

Dividing by 32, 32, 16 gives (7.1).

7.2 An exact annihilator

For $0 \leq j \leq 3$, let M_j be the matrix obtained by deleting column j from the exact matrix M . Define a functional $\ell : \mathcal{K} \rightarrow \mathbb{Q}_2$ by its coordinate vector

$$\ell_j = \frac{(-1)^j \det M_j}{2}.$$

All signed minors are divisible by 2 and at least one is not divisible by 4. Therefore ℓ is integral on $\mathcal{R}$ and primitive. Its certified residue is

$$\ell \equiv (28, 10, 173, 82) \pmod{256}. \quad (7.3)$$

The definition uses exact 2-adic minors, not minors of a truncated matrix. The congruence (7.1) determines (7.3) and proves independence of the three logarithms. By construction ℓ annihilates them. Since P, Q, R generate a subgroup of full rank modulo torsion, for every $Z \in E(K)$ a nonzero multiple lies in that subgroup. It follows that

$$\ell(\text{Log } Z) = 0 \quad (Z \in E(K)). \quad (7.4)$$

No determination of the odd index of H is needed.

Normalize $v_2(2) = 1$. Since $r = -1 + 2\alpha$, the residue (7.3) gives

$$v_2(\ell(1)) = 2, \quad v_2(\ell(r)) = 3. \quad (7.5)$$

One further congruence will exclude the mixed signs:

$$\ell(r \text{Log}(16P)) \equiv 128 \pmod{256}. \quad (7.6)$$

Indeed, $\text{Log}(16P)$ has coordinates $[96, 128, 128, 0]$ modulo 256. Multiplication by r gives $[160, 64, 128, 0]$, whose dot product with (7.3) is 128 modulo 256.

8 Rational parameters and completion of the proof

8.1 A local reduction for every rational parameter

Lemma 8.1. *If $T \in \mathbb{Q}$ and $(T, V) \in G(K)$, then $T \neq 0$ and $1/T \in 32\mathbb{Z}_2$.*

Proof. Set

$$A(T) = T^2 - 13T/4 + 2 = (T - a_+)(T - a_-).$$

Every factor of (3.2) is nonzero for rational T . The relative norms give

$$\begin{aligned} \left(\frac{N_{K/\mathbb{Q}(r)}(V)}{A(T)(T - b)} \right)^2 &= T^2 - 2, \\ \left(\frac{N_{K/\mathbb{Q}(s)}(V)}{A(T)(T - s)} \right)^2 &= T^2 + 7T + 2. \end{aligned} \tag{8.1}$$

Because 41 is 1 modulo 8, $\mathbb{Q}(r)$ embeds in $\mathbb{Q}_2$. Hence $T^2 - 2$ is a square in $\mathbb{Q}_2$. This is impossible for $T \in \mathbb{Z}_2$: for odd T it is 7 modulo 8, and for even T it has valuation 1. Thus $T \neq 0$ and $w = 1/T \in 2\mathbb{Z}_2$.

A rational 2-adic unit that is a square in $L = \mathbb{Q}_2(s)$ is already a square in $\mathbb{Q}_2$. Indeed, if $(c + ds)^2$ is rational with $c, d \in \mathbb{Q}_2$, then $cd = 0$. The possibility $c = 0$ would give the unit odd valuation $1 + 2v_2(d)$, a contradiction.

By the second norm identity,

$$U = 1 + 7w + 2w^2$$

is a square in L and a unit of $\mathbb{Q}_2$. Hence $U \equiv 1$ modulo 8. Since $U - 1 = w(7 + 2w)$ and the second factor is odd, $w \in 8\mathbb{Z}_2$.

Fix either embedding of K into L . Here $b \in \mathbb{Z}_2$ and

$$\begin{aligned} \frac{V^2}{T^4} &= \left(1 - \frac{13}{4}w + 2w^2 \right) \\ &\quad \cdot (1 - bw)(1 - sw). \end{aligned}$$

For $w \in 8\mathbb{Z}_2$, the last two factors are in $1 + 8\mathcal{O}_L$ and are squares by Hensel's lemma. Thus

$$C = 1 - \frac{13}{4}w + 2w^2$$

is a rational unit square in L , so $C \equiv 1$ modulo 8. But

$$C - 1 = \frac{w}{4}(-13 + 8w),$$

and the last factor is odd. Therefore $v_2(w) - 2 \geq 3$. □

8.2 The analytic identity on the whole disc

Set $w = 32t$ with $t \in \mathbb{Z}_2$, and define

$$\begin{aligned} F(w) &= (1 - a_+w)(1 - a_-w) \\ &\quad \cdot (1 - bw)(1 - sw) \\ &= \left(1 - \frac{13}{4}w + 2w^2 \right) \\ &\quad \cdot (1 - bw)(1 - sw). \end{aligned} \tag{8.2}$$

Its square root taking value 1 at zero is analytic in both factors of $\mathcal{K}$. In fact $F(32t) \in 1 + 8\mathcal{R}$, and the binomial series converges on the entire disc. The branch through P , denoted $Z_+(w)$, has coordinates

$$\begin{aligned} X(w) &= X_P \frac{1 - sw}{1 - bw}, \\ Y(w) &= Y_P \frac{\sqrt{F(w)}}{(1 - bw)^2}. \end{aligned} \tag{8.3}$$

Differentiation yields

$$\frac{dX}{2Y} = \frac{dw}{4\sqrt{F(w)}}.$$

Consequently, we seek the identity

$$\begin{aligned} \text{Log } Z_+(w) &= \text{Log } P + J(w), \\ J(w) &= \frac{1}{4} \int_0^w F(u)^{-1/2} du. \end{aligned} \tag{8.4}$$

To justify it on the entire disc, rather than only near zero, put

$$\begin{aligned} \kappa(w) &= \frac{X(w) - X_P}{Y(w) + Y_P} \\ &= \frac{w(1 - bw)}{2(\sqrt{F(w)} + (1 - bw)^2)}. \end{aligned}$$

This is analytic in t and belongs to $8\mathcal{R}$. The formal parameter of $Z_+(w) - P$, with its removable value at zero, is

$$-\frac{X(Z_+(w) - P)}{Y(Z_+(w) - P)} = \kappa \frac{N(w)}{D_0(w)},$$

where

$$\begin{aligned} N(w) &= 1 - (D + X(w) + X_P)\kappa^2, \\ D_0(w) &= 1 - (D + 2X(w) + X_P)\kappa^2 \\ &\quad + Y(w)\kappa^3. \end{aligned}$$

The denominator is a unit and the parameter lies in $8\mathcal{R}$. The formal logarithm therefore converges analytically throughout the disc. Its initial value and its differential prove (8.4).

Lemma 8.2. *Suppose $\lambda : \mathcal{K} \rightarrow \mathbb{Q}_2$ is linear, $\lambda(\mathcal{R}) \subseteq \mathbb{Z}_2$, and $\lambda(1) \in 4\mathbb{Z}_2$.*

There is a restricted power series $A_\lambda(t) \in \mathbb{Z}_2\langle t \rangle$ such that

$$\lambda(J(32t)) = 8\lambda(1)t + 64t^2 A_\lambda(t). \tag{8.5}$$

Here restricted means that the coefficients tend 2-adically to zero, so the series converges for every $t \in \mathbb{Z}_2$.

Proof. Write $F(32t)^{-1/2} = q(t)g(t)$, where

$$\begin{aligned} q(t) &= (1 - 104t + 2048t^2)^{-1/2}, \\ g(t) &= ((1 - 32bt)(1 - 32st))^{-1/2}. \end{aligned}$$

If $q(t) = \sum q_j t^j$ and $g(t) = \sum g_j t^j$, then $q_0 = g_0 = 1$ and, for $j \geq 1$,

$$v_2(q_j) \geq j + 1, \quad g_j \in 2^{3j+1}\mathcal{R}. \tag{8.6}$$

For the first estimate, use

$$1 - 104t + 2048t^2 = 1 + 8t(-13 + 256t).$$

Writing $s_2(k)$ for the number of nonzero binary digits of k , one has

$$v_2\binom{-1/2}{k} = -2k + s_2(k).$$

A degree j term in the power with exponent k has valuation at least

$$8j - 7k + s_2(k) \geq j + 1 \quad (1 \leq k \leq j).$$

Each factor of g has its degree $j \geq 1$ coefficient in $2^{3j+s_2(j)}\mathcal{R}$. Multiplication preserves the second bound in (8.6).

Now

$$J(32t) = 8 \int_0^t q(v)g(v) dv.$$

The linear term is $8t$. A term q_j with $j \geq 1$ acquires at least two further powers of 2 under λ , since q_j is rational. After integration its valuation is at least

$$3 + (j + 1) + 2 - v_2(j + 1) \geq 6.$$

For q_0g_j , with $j \geq 1$, the bound is $3 + 3j + 1 - v_2(j + 1) \geq 6$. For $q_i g_j$, with $i, j \geq 1$, it is $i + 3j + 5 - v_2(i + j + 1) \geq 6$. These bounds tend to infinity with the degree. Factoring out $64t^2$ proves the assertion. $\square$

8.3 Both relative sign patterns

The algebra $\mathcal{K}$ is the product of the two completions above 2. For $w \in 32\mathbb{Z}_2$, the two branches at each completion are (8.3) and its negative. Global negation identifies the four choices in pairs. It remains to treat equal and opposite signs.

For equal signs, (7.4) and (8.4) require $\ell(J(32t)) = 0$. By Lemma 8.2 and (7.5),

$$\begin{aligned} \ell(J(32t)) &= 32t(u_0 + 2tA(t)), \\ u_0 &\in \mathbb{Z}_2^*, \quad A(t) \in \mathbb{Z}_2\langle t \rangle. \end{aligned}$$

The second factor is a unit for every $t \in \mathbb{Z}_2$. Thus $t = 0$.

For opposite signs, let $\rho \in \mathbb{Q}_2$ be the value of r in the first completion. Its value in the second is $-\rho$, so multiplication by r/ρ represents the relative sign change. The necessary logarithmic equation, multiplied by 16, is

$$\ell(r \operatorname{Log}(16P)) + 16\ell(rJ(32t)) = 0. \tag{8.7}$$

Apply Lemma 8.2 to $\lambda(a) = \ell(ra)$. It is integral on $\mathcal{R}$ and has $v_2(\lambda(1)) = 3$. Therefore

$$\begin{aligned} 16\ell(rJ(32t)) &= 128\ell(r)t + 1024t^2 A_r(t) \\ &\in 1024\mathbb{Z}_2. \end{aligned}$$

But (7.6) makes the first term of (8.7) equal to 128 modulo 256. This case is impossible.

8.4 Conclusion

A point of $G(K)$ with finite rational parameter has $w = 1/T \in 32\mathbb{Z}_2$ by Lemma 8.1. Its image under (3.4) is covered by the two sign cases above. The only possible value is $w = 0$, which cannot equal $1/T$ for finite T . The two points at infinity do exist. This proves Theorem 3.2.

For a primitive solution of (1.1), Lemma 3.1 would supply a finite rational parameter $T = m/n$ if $n \neq 0$. Hence $n = 0$. Equation (2.3) and primitivity give

$$m = 1, \quad u^2 = 4, \quad v^2 = 1, \quad z^2 = 1.$$

Recovering $x = u + v$ and $y = u - v$ gives precisely the asserted signs and permutation of $(1, 3, 1)$. Homogeneity gives all nonprimitive solutions. If $z = 0$, then $x = y = 0$. This proves Theorem 1.1.

9 Further arithmetic of the elliptic curve

9.1 Selmer and Tate–Shafarevich groups

Proposition 9.1. *One has*

$$\begin{aligned}\mathrm{Sel}_2(E/K) &\cong (\mathbb{Z}/2\mathbb{Z})^5, \\ \mathrm{Sha}(E/K)[2^\infty] &= 0.\end{aligned}$$

Proof. Every Selmer class has even valuations outside S : by its local definition it lies in the local Kummer image, where the nonzero roots and root differences are units. The trivial class group of the ring of S -integers therefore represents its two components in the complete basis (4.2). Consequently,

$$\begin{aligned}E(K)/2E(K) &\subseteq \mathrm{Sel}_2(E/K), \\ \mathrm{Sel}_2(E/K) &\subseteq \mathcal{C}.\end{aligned}$$

The first and last spaces have dimension 5 by Sections 5–6, so both inclusions are equalities. The standard descent exact sequence identifies the quotient of $\mathrm{Sel}_2(E/K)$ by $E(K)/2E(K)$ with $\mathrm{Sha}(E/K)[2]$. Thus the latter is zero. Any nonzero element of order a power of 2 would yield an element of order 2 by multiplication, proving the second assertion without assuming finiteness of Sha . $\square$

9.2 Torsion

Proposition 9.2. *The full torsion subgroup is*

$$E(K)_{\mathrm{tors}} = E(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

In particular, as an abstract abelian group,

$$E(K) \cong \mathbb{Z}^3 \oplus (\mathbb{Z}/2\mathbb{Z})^2.$$

Proof. Use the degree-one primes specified by the residues below. The discriminant of (3.3) is $\Delta = 16B^2(D^2 - 4B)$.

Prime	Residue of r		Residue of s	
23	8		18	
31	14		8	

Prime	D	B	Δ	Number of points
23	3	7	8	28
31	18	11	14	40

Both reductions are good, and the point counts include infinity. Prime-to-residue-characteristic torsion injects into good reduction. Reduction at 31 excludes 23-primary torsion; reduction at 23 excludes 31-primary torsion. For every other prime both counts apply. The torsion order therefore divides $\gcd(28, 40) = 4$, and the four points of $E(K)[2]$ attain this bound. Proposition 6.1 gives the free rank. $\square$

These results do not determine the odd index of H , the odd-primary parts of Sha , or any special value of the associated L-function.

10 Reproducing the certificates

The two programs use only the Python 3 standard library. From the directory containing the two linked files, run

```
python3 verify_fermat_82.py
python3 verify_fermat_82_arithmetic.py
```

Do not use `-0` or `-00`, since assertions are part of the certificate checks. Both programs reject those modes and write their computed data to JSON files in the same directory.

`verify_fermat_82.py` checks the birational polynomial identity, the unit and norm certificates, the four finite local images, all 65536 global class pairs, the three points and their doublings, and the logarithmic residues (7.1)–(7.6). It uses the polynomial basis in θ for exact point arithmetic and reconstructs local conditions rather than assuming the list in Appendix B.

`verify_fermat_82_arithmetic.py` uses the separate basis $(1, r, s, rs)$. It verifies the ten identities in Appendix A, independence of the five Kummer codes, both finite-field point counts, and the logarithms at 64 and 80 bits of precision. All formal-logarithm terms required at each precision are included. Since their coefficients are integral at 2, terms of degree $2j + 1$ may be omitted modulo $2^N \mathcal{R}$ when $4(2j + 1) \geq N$.

These are finite arithmetic certificates, not a formalization of the entire proof. The completeness of the square-class basis, the dimensions of the local images, Lemma 8.1, and the analytic estimates are established in the text. No finite search bound for integer solutions, Birch–Swinnerton-Dyer conjecture, generalized Riemann hypothesis, or finiteness conjecture for Sha enters the argument.

Appendix A. Exact Kummer square identities

For an eight-bit mask m , put

$$g(m) = \prod_{j=0}^7 g_j^{m_j},$$

where m_j is its bit of index j and the generators are ordered as in (4.2). In row i , the Kummer component satisfies the exact identity

$$z = g(m)q_i^2.$$

The square roots are given in the second table.

Row	Component z	Mask m
1	$e_2 e_3$	33
2	$-e_2$	161
3	e_2	160
4	$e_2(e_2 - e_3)$	2
5	X_P	16
6	$X_P - e_2$	166
7	X_Q	0
8	$X_Q - e_2$	8
9	X_R	14
10	$X_R - e_2$	0

Row	Square root q_i
1	$[22, -3, -23, 5]$
2	$[6, -2, -2, 1]/2$
3	$[6, -2, -2, 1]/2$
4	$[22, -3, -23, 5]$
5	$[0, 0, 24, -7]/2$
6	$[63, -17, -26, 7]$
7	$[575, -155, -396, 104]/6$
8	$[899, -245, -723, 197]/6$
9	$[4584, -1242, -2690, 729]/28$
10	$[176, -74, -110, 27]/28$

The rows occur in pairs for T_0, T_2, P, Q, R . These are identities in K , not merely agreements of local square classes. Their masks give (6.2).

Appendix B. Coordinate conversion and binary restrictions

For $p_0 + p_1\theta + p_2\theta^2 + p_3\theta^3$, the four coordinates in $(1, \alpha, s, \alpha s)$ are

$$\begin{aligned} c_0 &= p_0 - p_1 + 43p_2 - 47p_3, \\ c_1 &= 2p_1 + 94p_3, \\ c_2 &= p_1 - 2p_2 + 125p_3, \\ c_3 &= 4p_2. \end{aligned}$$

Conversely, an element $[a, b, c, d]$ has polynomial-basis coordinates

$$\begin{aligned} p_0 &= a + b/2 - 43d/4, \\ p_1 &= (125b - 94c - 47d)/156, \\ p_2 &= d/4, \\ p_3 &= (-b + 2c + d)/156. \end{aligned}$$

Both descriptions give the same multiplication law using $\alpha^2 = \alpha + 10$, $s^2 = 2$, and the polynomial for θ .

One list of binary row masks defining $\mathcal{C}$ is

$$\begin{aligned} &8432, 5399, 720, 53271, 10, 161, 40960, 20896, \\ &64, 16384, 49392, 12528, 257, 171, 50432, 231. \end{aligned}$$

Each row is paired with the 16-bit class code by the dot product over $\mathbb{F}_2$. Their rank is 11 and their kernel is the span of (5.3).

References

- Ashleigh Ratcliffe and Bogdan Grechuk. *Generalised Fermat equation: a survey of solved cases*. arXiv:2412.11933v2, 14 April 2025, Section 2.1. Preprint.
- E. Victor Flynn and Joseph L. Wetherell. *Covering collections and a challenge problem of Serre*. Acta Arithmetica 98(2), 197–205, 2001. DOI.
- Christian Wüthrich. *Selmer groups*. Lecture notes, Baskerville Hall, August 2022, Section 2. Notes.