THE GENERALIZED FERMAT EQUATION $x^2 + y^5 = z^7$

MANVIR JASWAL

Abstract. We show that the equation $x^2 + y^5 = z^7$ has no solution in nonzero coprime integers, assuming a classification theorem from Putz's thesis, which has not appeared in a refereed journal. Equivalently, none of the equations $x^2 + y^5 = z^7$, $x^2 + y^7 = z^5$, $x^5 + y^7 = z^2$ has a solution in nonzero coprime integers. Putz attaches to a solution an octic algebra, the fibre of a Belyi map of degree 8, and proves that it is always isomorphic to one fixed octic field L_8. We prove unconditionally that no solution has fibre isomorphic to L_8, by a fifth-power descent over a field L_{24} of degree 24 that Putz introduced, completed by fifth-power residue symbols at five auxiliary primes. We also prove, without assuming the generalized Riemann hypothesis, that L_{24} has class number 1, using a criterion of Belabas, Diaz y Diaz and Friedman.

Contents

1. Introduction 1
2. Putz's theorem and the fields L_8 and L_{24} 6
3. The descent element and its norm 9
4. The valuations of E at the primes above 2 and 5 11
5. Auxiliary primes 14
6. The group $L_{24}(S, 5)$ 17
7. The sieve, and the proof of Theorem 1.1 18
8. A test on fibres where the descent element exists 20
Appendix A. The data of the sieve 21
Appendix B. The class number of L_{24} 30
Appendix C. Computations 34
Declarations 35
References 35

1. Introduction

1.1. **The equation.** For integers $p, q, r \geq 2$ the *generalized Fermat equation* of signature (p, q, r) is

$$x^p + y^q = z^r, \qquad \gcd(x, y, z) = 1, \qquad xyz \neq 0.$$

When $1/p + 1/q + 1/r < 1$, Darmon and Granville [8] proved that it has only finitely many solutions, and the Fermat–Catalan conjecture predicts that, taken over all such signatures together, there are only finitely many solutions in positive integers (counting $1 + 2^3 = 3^2$ once). Ten are known, and in each of them one exponent is 2 (see [2] and the survey [24]).

2020 *Mathematics Subject Classification.* Primary 11D41; Secondary 11R29, 11Y40, 11Y50.

Key words and phrases. Generalized Fermat equation, Fermat–Catalan conjecture, Belyi map, fifth-power descent, power residue symbols, class number, explicit formula.

This paper concerns the signature $(2,5,7)$. Ratcliffe and Grechuk [24, §1.1] note that, among the signatures (p,q,r) with p, q, r prime and $1/p+1/q+1/r<1$, it is the one with the smallest sum $p+q+r$ for which the equation was open.

Signatures whose exponents are three distinct primes form one of the main families of open cases. As Putz notes [23, p. 2], the only such signatures resolved when he wrote his thesis were $(2,3,7)$ [20] and, assuming the generalized Riemann hypothesis, $(2,3,11)$ [11]. For $(3,5,7)$, Dahmen and Siksek [6] resolve the equation under divisibility conditions, and the recent preprints of Chocian [4] and of the author [12] treat the whole equation. Both build on a classification due to Dahmen, Siksek and Putz, which the second states as a hypothesis. The modular method needs a Frey curve, and Frey elliptic curves are available for the signatures $(2,3,p)$ over $\mathbb{Q}$ and (q,q,r) over number fields [23, p. 3]. For other signatures Darmon's programme [7] would use Frey abelian varieties instead, but it depends on modularity results, and on large-image results for the associated Galois representations, that are not yet available [23, p. 2]. Putz instead works with a Belyi map, as we recall in Section 1.2.

We prove that $x^2+y^5=z^7$ has no solution in nonzero coprime integers, assuming Putz's reduction of the problem to a single number field (Theorem 2.2 below). Because two of the three exponents are odd, a solution of any one of

$$x^2+y^5=z^7, \qquad x^2+y^7=z^5, \qquad x^5+y^7=z^2$$

gives a solution of the others after changing signs and moving a term across the equation (for instance, $x^2+y^7=z^5$ is $x^2+(-z)^5=(-y)^7$). Following Putz [23], we write the equation as

$$X^5+Y^2=Z^7, \qquad \gcd(X,Y,Z)=1, \qquad XYZ\neq 0, \tag{1.1}$$

so that $(X,Y,Z)=(y,x,z)$ for a solution of $x^2+y^5=z^7$. A prime dividing two of X,Y,Z divides the third, so X,Y,Z are pairwise coprime. We call a triple of integers satisfying (1.1) a *solution*. Signs are allowed.

1.2. **Putz's reduction.** Put

$$\psi(t)=25t^3+20t^2+14t+14, \qquad \Psi(t)=10t^4+4t^3+2t^2+2t-1. \tag{1.2}$$

The rational function $\varphi(t)=4t^5\psi(t)/(4t-1)$ of degree 8 satisfies $\varphi(t)-1=\Psi(t)^2/(4t-1)$, because

$$4t^5\psi(t)-(4t-1)=\Psi(t)^2. \tag{1.3}$$

So, as a map $\mathbb{P}^1\to\mathbb{P}^1$, φ is ramified only above 0, 1 and ∞, with ramification indices $(5,1,1,1)$ above 0, $(2,2,2,2)$ above 1 and $(7,1)$ above ∞: it is a Belyi map adapted to the exponents 5, 2, 7. For a solution put

$$\eta=\frac{X^5}{Z^7}\in\mathbb{Q}\smallsetminus\{0,1\}, \qquad 1-\eta=\frac{Y^2}{Z^7}, \tag{1.4}$$

and let A_η be the fibre of φ above η, that is, the $\mathbb{Q}$-algebra

$$A_\eta=\mathbb{Q}[t]/(f_\eta), \quad f_\eta(t)=4t^5\psi(t)-\eta(4t-1)=100t^8+80t^7+56t^6+56t^5-4\eta t+\eta. \tag{1.5}$$

It has dimension 8 and is étale (Lemma 2.1), and it is unramified at every prime other than 2, 5 and 7 [23, Proposition 4.11]. Following the method of Darmon and Granville, Putz [23, Chapter 4] determines the possible completions of A_η at 2, 5 and 7, and at 3, where A_η is unramified but its possible completions still restrict the fields that can occur [23, Theorem 4.6]. He then excludes the cases in which A_η is not a field or has a subfield of degree 2 or 4 (using, among other tools, Chabauty's method on elliptic curves), and enumerates

the octic fields with the required local behaviour by targeted Hunter searches: enumerations of the polynomials whose coefficients satisfy the bounds that follow from Hunter's theorem and the congruences modulo powers of 2, 3, 5 and 7 that the required completions impose. The polynomials within Hunter's bounds include a defining polynomial of every primitive number field of a given degree and discriminant. The largest of these searches took about 46 000 hours of processor time [23, §3.7.1]. The outcome is his Theorem 4.33 (Theorem 2.2 below): for every solution, A_η is isomorphic to the field

$$\begin{gathered} L_8 = \mathbb{Q}(a), \qquad h(a) = 0, \\ h(x) = x^8 + 4x^7 - 28x^6 - 168x^5 - 140x^4 + 560x^3 + 840x^2 - 480x - 940. \end{gathered} \tag{1.6}$$

From this Putz derives congruence conditions on solutions, for example $5 \mid X$ and the absence of solutions with $2 \mid X$ or $4 \mid Z$ [23, Theorem 4.34 and Corollary 4.35]. He discusses three strategies for excluding L_8 and leaves each open [23, §4.5]. In a lecture in April 2025, Dahmen described partial resolutions for the signatures $(2, 5, 7)$ and $(3, 5, 7)$ under stringent congruence conditions, from work in part joint with Siksek and Putz [5].

1.3. **Main results.** Theorem 1.1 below is our main unconditional result. Theorem 1.2, which resolves the equation, combines it with Putz's theorem and is conditional on that theorem.

Let b be a root of ψ in an algebraic closure of L_8. The polynomial ψ is irreducible over L_8 (Lemma 2.4), so $L_{24} = L_8(b)$ is a field of degree 24.

Theorem 1.1. *Let (X, Y, Z) be a solution of (1.1). Then A_η is not isomorphic to L_8.*

The proof uses the fact that the class number of L_{24} is 1 (Theorem 6.1), which we prove in Appendix B without assuming the generalized Riemann hypothesis. Together with Putz's theorem, Theorem 1.1 gives:

Theorem 1.2. *Assume that for every solution of (1.1) the algebra A_η is isomorphic to L_8, as Putz's Theorem 4.33 [23] asserts (Theorem 2.2). Then the equation $x^2 + y^5 = z^7$ has no solution in nonzero coprime integers x, y, z. Equivalently, none of the equations $x^2 + y^5 = z^7$, $x^2 + y^7 = z^5$ and $x^5 + y^7 = z^2$ has a solution in nonzero coprime integers.*

Proof. By hypothesis, a solution of (1.1) has $A_\eta \simeq L_8$, which Theorem 1.1 excludes. The equivalent forms follow from Section 1.1. □

1.4. **The idea of the proof.** Suppose that $A_\eta \simeq L_8$, and let $\theta \in L_8$ be the image of the class of t, so that $f_\eta(\theta) = 0$, that is,

$$4\theta^5\psi(\theta) = \eta\,(4\theta - 1). \tag{1.7}$$

Since $\eta = X^5/Z^7$, (1.7) says that $\theta^5\psi(\theta) = X^5(4\theta - 1)/(4Z^7)$. Over L_{24} the factor $\theta - b$ of $\psi(\theta)$ becomes available, and the descent studies it modulo fifth powers, through the element

$$E = 80000\,(\theta - b)\,\psi(\theta)^3 \in L_{24}. \tag{1.8}$$

The constant $80000 = 2^7 \cdot 5^4$ only normalizes E. Its factor 5^4 cancels, up to fifth powers, the denominator 25 of $\mathrm{N}_{L_{24}/L_8}(\theta - b) = \psi(\theta)/25$ (see (2.1)), since $80000^3/25 = 2^{21} \cdot 5^{10}$ (Proposition 3.2). Its factor 2^7 is a choice of normalization, with which the norm of E is 2 times a fifth power. Any other power of 2, or any other nonzero rational constant, would serve equally well: it would change the class of E by a fixed class, and the conditions below accordingly.

The proof has four steps.

(1) *Descent* (Section 3). Because X and Z are coprime, the valuation of E at every prime of L_{24} not above 2, 5 or 7 is divisible by 5 (Proposition 3.1). So the class of E lies in the finite group $L_{24}(S,5)$ of classes in $L_{24}^{\times}/L_{24}^{\times 5}$ with this property, where S is the set of primes of L_{24} above 2, 5 and 7. Moreover, for every $\theta \in L_8$ the norm of E to L_8 is 2 times a fifth power (Proposition 3.2). This is the reason for the factor $\psi(\theta)^3$: up to a constant it is the cube of the norm of $\theta - b$, and for any element u of a cubic extension, $u \cdot \mathrm{N}(u)^3$ has norm $\mathrm{N}(u)^{10}$, a fifth power.

(2) *Local conditions at* 2 *and* 5 (Section 4). The field L_{24} has a single prime above 2, and it is totally ramified (Lemma 2.5). There the valuation of E is 3 modulo 5 for every $\theta \in L_8$, a consequence of the norm identity (Lemma 4.1). At the seven primes above 5 the valuations of E modulo 5 are $2, 3, 0, 0, 0, 0, 0$ for every solution (Proposition 4.2). Because θ generates L_8, the factorization of f_η over $\mathbb{Q}_5$ must match the decomposition of 5 in L_8, and Newton polygons then determine the valuations. The proof also shows $5 \nmid YZ$.

(3) *Auxiliary primes* (Section 5). If a prime $q \notin \{2, 5, 7\}$ divides XYZ, then η reduces modulo q to one of the branch points 0, ∞, 1 of φ, and the splitting of A_η at q is then of one of three restricted kinds, read off from the factorizations modulo q of ψ, of binomials $s^5 - c$ and $s^7 - c$, and of Ψ (Proposition 5.2). A search of the primes $q \equiv 1 \pmod 5$ up to 700, for which $\mathbb{F}_q$ contains the fifth roots of unity, finds sixteen at which the splitting of L_8 is of none of these kinds, so that $q \nmid XYZ$. Then the residues of θ at the primes of L_8 above q are roots of the reduction of f_η modulo q, which depends only on η mod q. Running through all values of η mod q and all such roots gives a finite set $I(q)$ that must contain the vector of fifth-power residue symbols of E at the primes of L_{24} above q (Proposition 5.3).

(4) *The sieve* (Sections 6 and 7). Since the class number of L_{24} is 1 (Theorem 6.1), $L_{24}(S,5)$ is the group of S-units of L_{24} modulo fifth powers. It has dimension $24 = r_1 + r_2 - 1 + \#S$ over $\mathbb{F}_5$, where $(r_1, r_2) = (2, 11)$ is the signature of L_{24} and $\#S = 12$, and Table 4 gives a basis of it consisting of S-units. The norm condition cuts the possible classes of E to an affine subspace of dimension 14, and the valuations at the primes above 5 cut it to dimension 10. The sieve then uses the conditions at the five auxiliary primes with the smallest proportion $\#I(q)/5^m$, where m is the number of primes of L_{24} above q. Taken in turn, $q = 181, 311, 131, 251, 101$ leave 36 875, 567, 19, 1 and 0 classes (Theorem 7.1).

The last step is a finite computation over $\mathbb{F}_5$, and all of its data are printed in Appendix A.

That five primes are enough is not surprising. At an auxiliary prime q the norm condition ties together the symbols of E above each prime of L_8, so on the affine subspace of dimension 10 the vector of symbols at q takes at most $5^{m-m'}$ values, where m' is the number of primes of L_8 above q. At the five primes used it takes exactly $5^{m-m'}$ values, and the fraction of these that lie in $I(q)$ ranges from $59/5^6$ at $q = 181$ to $16/5^4$ at $q = 101$. If the five conditions were independent, the expected number of surviving classes would be about 0.001 (Remark 7.3).

Section 8 applies the same computation to the fibres of φ above two rational points of the twisted equation $X^5 + 2Y^2 = Z^7$ ($\eta = -1$ and $\eta = 243$). Each of these fibres is an octic field K_8 not isomorphic to L_8, and over $K_{24} = K_8(b)$ the element defined as in (1.8) exists, so its class must satisfy every condition. The sieve keeps exactly one class, the class of E. This tests the conditions and their implementation on fibres where the answer is known.

1.5. **Relation to earlier work.** The field L_{24}, and the idea of a factorization into fifth powers over it, are due to Putz. In [23, §4.5.2, pp. 150–152] he considers the compositum of L_8

with the cubic field $\mathbb{Q}[U]/(U^3+8U^2+56U+560)$. Since $U^3+8U^2+56U+560 = 40\,\psi(U/10)$, this is L_{24}, with $10b$ as the root of the cubic. Putz writes r for our θ, and θ for $10b$. For a solution with $A_\eta \simeq L_8$ he puts $w = 10\theta Z$ [23, Lemma 4.38] and divides w and Z by their greatest common divisor in L_8 to obtain w_0, z_0. He shows that the cubic form $g(U,V) = U^3 + 8U^2V + 56UV^2 + 560V^3$ satisfies $g(w_0, z_0) = \alpha y_0^5$, with α and y_0 in the ring of integers of L_8 and α divisible only by primes above 2, 5 and 7 [23, Proposition 4.39]. This uses $5 \mid X$ and the triviality of the class group of L_8. Assuming that the class group of L_{24} is trivial, and remarking that a class number prime to 5 may suffice, he writes the linear factor $g_1(w_0, z_0) = w_0 - 10bz_0$ as $\alpha_1\beta_1^5$, with α_1 divisible only by primes above 2, 5 and 7. He thereby reduces the problem to rational points on finitely many curves of genus 2 over L_{24}, a route he did not pursue. Our element is closely related to his: $E = g_1(w, Z)\, g(w, Z)^3/(8Z^{10})$, so that, modulo fifth powers, E is $4\, g_1(w_0, z_0)\, g(w_0, z_0)^3$ (Remark 3.3).

What is new here is the following.

(i) The factor $\psi(\theta)^3$, which makes the norm of E a known class, the class of 2 in $L_8^\times/L_8^{\times 5}$ (Proposition 3.2). In Putz's normalization the norm of $g_1(w_0, z_0)$ is $g(w_0, z_0) = \alpha y_0^5$, whose class, that of α, is unknown.

(ii) A direct proof that the class of E lies in $L_{24}(S, 5)$ (Proposition 3.1), which uses only that X and Z are coprime: it needs neither the class number of L_8 nor $5 \mid X$.

(iii) The valuations of E at the primes above 2 and 5 (Section 4), derived from the isomorphism $A_\eta \simeq L_8$ alone, without Putz's congruence conditions.

(iv) The use of auxiliary primes in the descent. Putz used his local description of A_η at primes dividing XYZ (Proposition 5.2) to exclude $q \mid XYZ$ and restrict η modulo q for $q = 11$ and 197 [23, Theorem 4.34(v),(vi)]. Here the same description restricts the fifth-power residue symbols of E at sixteen primes, and a computation eliminates every class (Sections 5, 6 and 7).

(v) A proof, without the generalized Riemann hypothesis, that L_{24} has class number 1 (Appendix B), which Putz assumed in the approach recalled above.

Our proof of Theorem 1.1 is a descent of a familiar kind: the class of E lies in a finite group, local conditions cut out a subset of it, and one shows that this subset is empty. For the descent map on cyclic covers of the projective line see Poonen and Schaefer [19]. In the partial descent of Siksek and Stoll [25] for $x^3 + y^4 + z^5 = 0$ and the two-cover descent of Bruin and Stoll [3], sets of this kind are shown to be empty in order to prove that a curve has no rational points. They also appear in the working paper of Dahmen and Siksek on $x^5 + y^3 = z^7$ [6]. As in those descents, the norm class of E is known in advance, so that the norm gives a fixed affine condition. The same finishing method, a fifth-power descent completed by residue symbols at auxiliary primes, is used in our treatment of $x^5+y^3 = z^7$ [12, §3], for a septic field left by the reduction there.

1.6. **The inputs of the proof.** The proof of Theorem 1.2 rests on the following.

(i) Putz's Theorem 4.33 [23] (Theorem 2.2). It is part of a doctoral thesis and has not appeared in a refereed journal. Its proof rests on local computations and elliptic-curve Chabauty computations in Magma, and on Hunter searches run with a C++ program, none of which we have repeated. Putz's Magma scripts for the proofs of his Chapter 4, with their outputs, are public [21], and so is his program for the Hunter searches [22]. The scripts do not ask Magma for class group bounds that assume the generalized Riemann hypothesis. They compute 2-Selmer groups, rank bounds and Mordell–Weil

subgroups of elliptic curves over number fields, which rest on class group and unit computations, and neither the thesis nor the scripts say whether these were proved. The repository of these scripts names Magma V2.28-8 as compatible, and Elsenhans and Voight report that for some time before V2.29 a bug disabled the saturation step with which Magma's default class group computation confirms its result, although they consider it unlikely that a wrong answer was returned [9].

(ii) A criterion of Belabas, Diaz y Diaz and Friedman [1, Theorem 5.1], deduced from Weil's explicit formula [26] in the form given by Poitou [18], under which the prime ideals of small norm generate the class group of a number field. It assumes no hypothesis on the zeros of L-functions [1, §5]. With it and with computations of the kind described in (iii), we prove in Appendix B that the class number of L_{24} is 1 (Theorem 6.1).

(iii) Explicit computations with PARI/GP [17] and Python. Each is stated in the text as a numbered lemma, proposition, theorem or displayed identity, or as one of the steps (a)–(c) of Appendix B.2. The data of the sieve are printed in Appendix A, and the coefficients used for Theorem 6.1 in Table 9. The generators of the 665 770 prime ideals of Appendix B are too many to print, and the deposited programs [14] find each of them again and check it as in Appendix B.2(c), in about an hour. Appendix C lists the computations and says which were repeated by separately written programs.

Theorems 1.1 and 1.2 have been formalized in Lean 4 with Mathlib [13], following the proof given here, with Theorem 7.1 checked from the data printed in Appendix A. The formal statements take two hypotheses: Putz's theorem, for Theorem 1.2 only, and the absence of elements of order 5 in the class group of L_{24}, a consequence of Theorem 6.1, whose proof in Appendix B is not formalized. The formal proofs use only Lean's standard axioms.

1.7. **Plan of the paper.** Section 2 states Putz's theorem and describes the fields L_8 and L_{24}. Section 3 shows that the class of E lies in $L_{24}(S,5)$ and computes its norm to L_8, Section 4 computes the valuations of E at the primes above 2 and 5, and Section 5 gives the conditions at the auxiliary primes. Section 6 describes the group $L_{24}(S,5)$ and states the class number of L_{24}, and Section 7 carries out the sieve and proves Theorem 1.1. Section 8 shows, on two fibres of φ above points of a twisted equation, that the conditions keep a class that exists. Appendix A prints the data, Appendix B proves that the class number of L_{24} is 1, and Appendix C describes the computations. Table 1 lists the main notation.

2. Putz's theorem and the fields L_8 and L_{24}

This section states Putz's theorem and collects the facts about L_8 and L_{24} that the later sections use: their degrees, signatures and discriminants (Lemma 2.4), the primes of L_{24} above 2, 5 and 7 (Lemma 2.5), and the roots of ψ over $\mathbb{Q}_5$ (Lemma 2.6), on which the 5-adic computations of Section 4 rest.

2.1. **The fibre algebra.** We keep the notation ψ, Ψ, f_η, A_η of (1.2)–(1.5). For a variable s put $f_s(t) = 4t^5\psi(t) - s(4t-1)$.

Lemma 2.1. *The discriminant of f_s with respect to t is $-2^{28}\cdot 5^{12}\cdot 7^7\cdot s^4(s-1)^4$. In particular, for $\eta \in \mathbb{Q}\smallsetminus\{0,1\}$ the polynomial f_η is separable of degree 8, and A_η is an étale $\mathbb{Q}$-algebra of dimension 8.*

Proof. A direct computation (Appendix C) gives this formula, which agrees with [23, Lemma 4.4]. The leading coefficient of f_s is 100, so f_η has degree 8. For $\eta \notin \{0,1\}$

Symbol	Meaning
X, Y, Z	a solution of (1.1); $(X, Y, Z) = (y, x, z)$ for $x^2 + y^5 = z^7$
η	X^5/Z^7
$\psi,\ \Psi$	$25t^3 + 20t^2 + 14t + 14$ and $10t^4 + 4t^3 + 2t^2 + 2t - 1$, with $4t^5\psi - (4t-1) = \Psi^2$
$f_\eta,\ A_\eta$	$4t^5\psi(t) - \eta(4t-1)$; the algebra $\mathbb{Q}[t]/(f_\eta)$
$h,\ a,\ L_8$	the octic polynomial (1.6); a root of h; the field $\mathbb{Q}(a)$
θ	the root of f_η in L_8 given by an isomorphism $A_\eta \simeq L_8$
$b,\ L_{24}$	a root of ψ; the field $L_8(b)$ of degree 24
E	$80000(\theta - b)\psi(\theta)^3 \in L_{24}$
S	the twelve primes $\mathfrak{P}_1, \dots, \mathfrak{P}_{12}$ of L_{24} above 2, 5, 7 (Table 2)
$L_{24}(S, 5)$	classes in $L_{24}^\times / L_{24}^{\times 5}$ with valuation divisible by 5 at every prime outside S
$B_1, \dots, B_{24}$	the basis of $L_{24}(S, 5)$ (Proposition 6.2, Table 4)
$u_1, \dots, u_{10}$	S-units of L_8 used for the norm condition (Table 5)
$\mathsf{N},\ \mathsf{T}$	the norm matrix and the coordinate vector of 2 (Section 6.3)
$\mathcal{Q}$	the sixteen auxiliary primes (Proposition 5.4)
$\chi_{\mathfrak{Q}}$	the fifth-power residue symbol at a prime $\mathfrak{Q}$ of L_{24}, with values in $\mathbb{F}_5$
$I(q),\ M_q$	the allowed symbol vectors of E at q; the symbols of $B_1, \dots, B_{24}$ at q

TABLE 1. Main notation.

the discriminant is nonzero, so f_η is separable, and a separable polynomial defines an étale algebra. □

A solution of (1.1) in our sense is what Putz [23, §1.1 and §4.1] calls a nontrivial solution, written (x, y, z) there. He attaches to it $\eta = X^5/Z^7$ and the algebra $\mathbb{Q}[t]/(\varphi_0(t) - \eta\varphi_\infty(t))$ with $\varphi_0(t) = 4t^5\psi(t)$ and $\varphi_\infty(t) = 4t - 1$, which is our A_η, and proves:

Theorem 2.2 (Putz [23, Theorem 4.33, p. 141])**.** *Let (X, Y, Z) be a solution of (1.1). Then A_η is isomorphic to the field $L_8 = \mathbb{Q}[x]/(h(x))$ of (1.6).*

Remark 2.3. This is the only result of [23] that we use. The congruence conditions of [23, Theorem 4.34 and Corollary 4.35] play no role: Proposition 4.2 below recovers $5 \nmid YZ$ from the isomorphism $A_\eta \simeq L_8$ alone, and the valuation of E at the prime above 2 follows from the norm identity of Proposition 3.2 (Lemma 4.1).

The thesis states its 2-adic conditions twice, and the two statements differ. In its cases (a) and (b), [23, Theorem 4.2(i)] has $Z \equiv 3$ and $Z \equiv 7 \pmod 8$, where [23, Theorem 4.34(i)] has $Z \equiv 5$ and $Z \equiv 1 \pmod 8$. The proof of [23, Theorem 4.34(i)] describes the two cases by $v_2(1-\eta) = 2$ with $1 - \eta \equiv 5$ modulo squares, and by $v_2(1-\eta) \geq 4$ with $1 - \eta \equiv 1$ modulo squares. In both cases $v_2(1-\eta) > 0$, so Z is odd, because $1 - \eta = Y^2/Z^7$ and Y, Z are coprime. Then $1 - \eta$ is Z times a square in $\mathbb{Q}_2$, and the two cases give $Z \equiv 5$ and $Z \equiv 1 \pmod 8$, as in [23, Theorem 4.34(i)]. So the congruences in [23, Theorem 4.2(i)] appear to be misprints.

2.2. **The fields.** Let a be a root of h, so that $L_8 = \mathbb{Q}(a)$, and let b be a root of ψ in an algebraic closure of L_8.

Lemma 2.4. (a) *The polynomial h is irreducible. The field L_8 has signature $(2, 3)$ and discriminant $-2^{14} \cdot 5^6 \cdot 7^7$, and the index of $\mathbb{Z}[a]$ in the ring of integers of L_8 is $2^7 \cdot 5 \cdot 41$.*

(b) *The primes 2, 5, 7 factor in L_8 as*

$$2 = \mathfrak{p}_2^8, \qquad 5 = \mathfrak{p}_A^5\,\mathfrak{p}_B\,\mathfrak{p}_C^2, \qquad 7 = \mathfrak{p}_7\,\mathfrak{p}_7'^7,$$

where all the primes shown have residue degree 1.

(c) *The polynomial* ψ *is irreducible over* L_8*. Hence* $L_{24} = L_8(b)$ *has degree* 24*, and for* $t \in L_8$

$$\mathrm{N}_{L_{24}/L_8}(t-b) = (t-b_1)(t-b_2)(t-b_3) = \psi(t)/25, \tag{2.1}$$

where b_1, b_2, b_3 *are the roots of* ψ*.*

(d) *The field* L_{24} *has signature* $(2, 11)$ *and discriminant* $-2^{44} \cdot 5^{20} \cdot 7^{23}$*. The element* $5b$ *is an algebraic integer, a root of* $x^3 + 4x^2 + 14x + 70$*.*

Proof. Parts (a), (b) and the discriminant in (d) are computations with PARI/GP, listed in Appendix C: `nfinit` and `idealprimedec` compute the rings of integers and the prime decompositions, and `nfcertify` proves that the computed integral bases are bases of the rings of integers (we then call the maximal orders certified). For (c): the coefficients 20, 14, 14 of ψ are even, 14 is not divisible by 4 and 25 is odd, so ψ is Eisenstein at 2 and $\mathbb{Q}(b)$ is a cubic field. If ψ were reducible over L_8, it would have a root there, and the cubic field $\mathbb{Q}(b)$ would be a subfield of the octic field L_8, which is impossible as $3 \nmid 8$. Since the roots of ψ are the conjugates of b over L_8, (2.1) follows. For (d): ψ has negative discriminant $-2^2 \cdot 5^7 \cdot 7$, so it has one real root. Each of the two real embeddings of L_8 therefore extends to exactly one real embedding of L_{24}, and L_{24} has 2 real and $(24-2)/2 = 11$ pairs of complex embeddings. Finally $5\,\psi(x/5) = x^3 + 4x^2 + 14x + 70$. □

We will use the following norms from $\mathbb{Q}(b)$ to $\mathbb{Q}$, all read off from ψ (or its resultants):

$$\mathrm{N}(b) = -\tfrac{14}{25}, \qquad \mathrm{N}(1-4b) = \tfrac{64\,\psi(1/4)}{25} = 49, \qquad \mathrm{N}(\psi'(b)) = 2^2 \cdot 5^5 \cdot 7, \tag{2.2}$$

together with $\psi(0) = 14$ and $\psi(1/4) = 5^2 \cdot 7^2/2^6$.

2.3. **The primes of L_{24} above 2, 5 and 7.** For a prime $\mathfrak{P}$ of L_{24} above a rational prime p, with $\mathfrak{p} = \mathfrak{P} \cap L_8$, we call the triple

$$(e(\mathfrak{P}/p),\ f(\mathfrak{P}/p),\ e(\mathfrak{p}/p))$$

the *label* of $\mathfrak{P}$.

Lemma 2.5. *There are twelve primes of* L_{24} *above* 2, 5 *and* 7*, with the following labels:*

p	*labels of the primes of* L_{24} *above* p
2	$(24, 1, 8)$
5	$(1, 1, 1)$, $(2, 1, 1)$, $(5, 1, 5)$, $(10, 1, 5)$, *and* $(2, 1, 2)$ *three times*
7	$(1, 1, 1)$, $(2, 1, 1)$, $(7, 1, 7)$, $(14, 1, 7)$

In particular the prime $\mathfrak{p}_C$ *of* L_8 *above* 5 *splits into three primes of* L_{24}*, each of ramification index and residue degree* 1 *over* $\mathfrak{p}_C$*. So* ψ *splits completely over the completion* $L_{8,\mathfrak{p}_C}$*.*

Proof. The labels are computed by `idealprimedec` (Appendix C). They can also be seen by hand from the local structure of ψ and L_8. Since $L_{24} = L_8 \otimes_{\mathbb{Q}} \mathbb{Q}(b)$, for each prime p we have $L_{24} \otimes \mathbb{Q}_p = (L_8 \otimes \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} (\mathbb{Q}(b) \otimes \mathbb{Q}_p)$. At 2, ψ is Eisenstein and $L_8 \otimes \mathbb{Q}_2$ is a totally ramified field of degree 8. The ramification indices 3 and 8 are coprime, so the tensor product is a field with $e = 24$. At 5, $\mathbb{Q}(b) \otimes \mathbb{Q}_5 = \mathbb{Q}_5 \times \mathbb{Q}_5(b_2)$ with $\mathbb{Q}_5(b_2)$ ramified quadratic (Lemma 2.6 below), and $L_8 \otimes \mathbb{Q}_5 = L_{8,\mathfrak{p}_A} \times L_{8,\mathfrak{p}_B} \times L_{8,\mathfrak{p}_C}$ with $L_{8,\mathfrak{p}_B} = \mathbb{Q}_5$ and $L_{8,\mathfrak{p}_A}$, $L_{8,\mathfrak{p}_C}$ totally ramified of degrees 5 and 2. The factors are $L_{8,\mathfrak{p}_B} \otimes \mathbb{Q}_5$ (label $(1,1,1)$), $L_{8,\mathfrak{p}_B} \otimes \mathbb{Q}_5(b_2)$ (label $(2,1,1)$), $L_{8,\mathfrak{p}_A} \otimes \mathbb{Q}_5$ (label $(5,1,5)$), $L_{8,\mathfrak{p}_A} \otimes \mathbb{Q}_5(b_2)$ (a field with $e = 10$, label $(10,1,5)$), $L_{8,\mathfrak{p}_C} \otimes \mathbb{Q}_5$ (label $(2,1,2)$), and $L_{8,\mathfrak{p}_C} \otimes \mathbb{Q}_5(b_2)$. For the last one, $L_{8,\mathfrak{p}_C} \simeq \mathbb{Q}_5(b_2)$, so it is a product of two fields, each isomorphic to $L_{8,\mathfrak{p}_C}$ (as the labels computed by `idealprimedec`

also show). Indeed, $h(y-3) = y^8 - 20y^7 + 140y^6 - 420y^5 + 490y^4 - 28y^3 - 420y^2 + 420y - 175$ has 5-adic Newton polygon with vertices $(0,2)$, $(1,1)$, $(3,0)$, $(8,0)$, so its two roots of valuation $1/2$, which generate $L_{8,\mathfrak{p}_C}$, satisfy $y^2 = 15u$ with $u \equiv 1$ modulo the maximal ideal (the terms $420y$ and $-28y^3$ dominate), and $L_{8,\mathfrak{p}_C} = \mathbb{Q}_5(\sqrt{15})$; and since $b_1 \in \mathbb{Q}_5$ and $\operatorname{disc}\psi = 25^2\psi'(b_1)^2(b_2-b_3)^2$, we have $\mathbb{Q}_5(b_2) = \mathbb{Q}_5(\sqrt{\operatorname{disc}\psi}) = \mathbb{Q}_5(\sqrt{-35}) = \mathbb{Q}_5(\sqrt{15})$, because $-35/15 = -7/3 \equiv 1 \pmod 5$ is a square in $\mathbb{Q}_5$. At 7, ψ has one root in $\mathbb{Z}_7$ and two roots generating a ramified quadratic extension, and $L_8 \otimes \mathbb{Q}_7$ is the product of $\mathbb{Q}_7$ and a totally ramified field of degree 7. The four products give the four labels. □

We number the twelve primes $\mathfrak{P}_1, \dots, \mathfrak{P}_{12}$ as in Table 2. Each $\mathfrak{P}_i$ is generated by the element B_i of Table 4 (Proposition 6.2(i)). The two primes above 5 with labels $(1,1,1)$ and $(2,1,1)$ are $\mathfrak{P}_3$ and $\mathfrak{P}_5$.

prime	p	label	prime	p	label
$\mathfrak{P}_1$	2	$(24,1,8)$	$\mathfrak{P}_7$	5	$(5,1,5)$
$\mathfrak{P}_2$	5	$(2,1,2)$	$\mathfrak{P}_8$	5	$(2,1,2)$
$\mathfrak{P}_3$	5	$(1,1,1)$	$\mathfrak{P}_9$	7	$(1,1,1)$
$\mathfrak{P}_4$	5	$(2,1,2)$	$\mathfrak{P}_{10}$	7	$(7,1,7)$
$\mathfrak{P}_5$	5	$(2,1,1)$	$\mathfrak{P}_{11}$	7	$(14,1,7)$
$\mathfrak{P}_6$	5	$(10,1,5)$	$\mathfrak{P}_{12}$	7	$(2,1,1)$

TABLE 2. The primes $\mathfrak{P}_i = B_i\mathcal{O}_{L_{24}}$ of L_{24} above 2, 5 and 7 and their labels $(e(\mathfrak{P}_i/p), f(\mathfrak{P}_i/p), e(\mathfrak{P}_i \cap L_8/p))$.

From now on v_5 denotes the valuation on an algebraic closure of $\mathbb{Q}_5$ with $v_5(5) = 1$.

Lemma 2.6. *Over $\mathbb{Q}_5$, the polynomial ψ has exactly one root $b_1 \in \mathbb{Z}_5$; it satisfies $b_1 \equiv -1 \pmod 5$, $v_5(4b_1 - 1) = 2$ and $v_5(\psi'(b_1)) = 0$. The other two roots b_2, b_3 have $v_5(b_2) = v_5(b_3) = -1$ and $v_5(b_2 - b_3) = 3/2$, and $\mathbb{Q}_5(b_2) = \mathbb{Q}_5(b_3)$ is a ramified quadratic extension of $\mathbb{Q}_5$.*

Proof. The 5-adic valuations of the coefficients of ψ at t^0, t^1, t^2, t^3 are $0, 0, 1, 2$, so the Newton polygon has vertices $(0,0)$, $(1,0)$, $(3,2)$: one root of valuation 0 and two of valuation -1. Modulo 5, $\psi \equiv 14(t+1)$, so the unit root is a simple root modulo 5, lies in $\mathbb{Z}_5$ by Hensel's lemma, and is $\equiv -1$. Since $\prod_i(1-4b_i) = 49$ is a 5-adic unit and $v_5(1-4b_2) = v_5(1-4b_3) = -1$, we get $v_5(1-4b_1) = 2$. Next, $\psi'(b_1) = 25(b_1-b_2)(b_1-b_3)$ has valuation $2-1-1 = 0$. From $\operatorname{disc}\psi = -2^2 \cdot 5^7 \cdot 7 = 25^4 \prod_{i<j}(b_i - b_j)^2$ we get $7 = 8 + 2(-1 - 1 + v_5(b_2 - b_3))$, so $v_5(b_2 - b_3) = 3/2$. As $b_3 = -4/5 - b_1 - b_2 \in \mathbb{Q}_5(b_2)$ and $v_5(b_2 - b_3) \notin \mathbb{Z}$, the extension $\mathbb{Q}_5(b_2)/\mathbb{Q}_5$ is ramified of degree 2. □

3. The descent element and its norm

A solution with $A_\eta \simeq L_8$ gives an element E of L_{24} whose class modulo fifth powers lies in a finite group $L_{24}(S,5)$ (Proposition 3.1) and whose norm to L_8 is 2 times a fifth power (Proposition 3.2). The first fact reduces the problem to finitely many classes, and the second gives the norm condition (N) of Section 7.

Let S be the set of the twelve primes of L_{24} above 2, 5 and 7, and let

$$L_{24}(S,5) = \{\alpha \in L_{24}^\times / L_{24}^{\times 5} \ : \ v_{\mathfrak{P}}(\alpha) \equiv 0 \pmod 5 \text{ for every prime } \mathfrak{P} \notin S\}, \tag{3.1}$$

where $v_{\mathfrak{P}}$ is the normalized valuation of $\mathfrak{P}$ ($v_{\mathfrak{P}}(L_{24}^{\times}) = \mathbb{Z}$). The group $L_{24}(S,5)$ is a finite-dimensional vector space over $\mathbb{F}_5$ (Section 6).

Suppose (X,Y,Z) is a solution with $A_\eta \simeq L_8$. Fix such an isomorphism and let $\theta \in L_8$ be the image of the class of t. Then θ generates L_8, and (1.7) holds. The next proposition uses much less: only coprime nonzero integers X, Z and a root θ of f_η in a number field containing b. Section 8 uses this generality.

Proposition 3.1. *Let X, Z be coprime nonzero integers and $\eta = X^5/Z^7$. Let K be a number field containing b and an element θ with $f_\eta(\theta) = 0$, and put $E = 80000(\theta - b)\psi(\theta)^3 \in K$. Then:*

(i) *$\psi(\theta) \neq 0$ and $\theta \neq b$, so $E \neq 0$;*

(ii) *$v_{\mathfrak{P}}(E) \equiv 0 \pmod 5$ for every prime $\mathfrak{P}$ of K not above 2, 5 or 7;*

(iii) *$v_{\mathfrak{P}}(E) = 0$ for every prime $\mathfrak{P}$ of K above a prime $p \notin \{2,5,7\}$ with $p \nmid XZ$.*

In particular, if (X,Y,Z) is a solution with $A_\eta \simeq L_8$ and $\theta \in L_8$ is as above, then the class of E lies in $L_{24}(S,5)$.

Proof. Since $f_\eta(\theta) = 0$, the element θ satisfies (1.7). (i) If $\psi(\theta) = 0$ then (1.7) gives $\eta(4\theta - 1) = 0$, so $\theta = 1/4$. But $\psi(1/4) = 5^2 \cdot 7^2/2^6 \neq 0$. Hence $\psi(\theta) \neq 0$, and so $\theta \neq b$.

For (ii) and (iii), let $\mathfrak{P}$ be a prime of K above $p \notin \{2,5,7\}$, write $v = v_{\mathfrak{P}}$ and $e = v(p)$. Since $5b$ is integral and $p \neq 5$, b is $\mathfrak{P}$-integral, and so are $1 - 4b$ and $\psi'(b)$. Their norms to $\mathbb{Q}$ in (2.2) are prime to p, so all three are units at every prime above p: an element that is integral at every prime above p and whose norm is prime to p is a unit at each of these primes. Write $\psi(t) = 25(t - b)\psi_1(t)$, where

$$\psi_1(t) = t^2 + (b + \tfrac{4}{5})t + (b^2 + \tfrac{4}{5}b + \tfrac{14}{25}) \in \mathbb{Q}(b)[t]$$

has $\mathfrak{P}$-integral coefficients and $\psi_1(b) = \psi'(b)/25$, a $\mathfrak{P}$-unit. Finally $v(\eta) = e\,(5v_p(X) - 7v_p(Z))$, and at most one of $v_p(X)$, $v_p(Z)$ is positive.

Case $p \nmid Z$. Then $v(\eta) = 5e\,v_p(X) \geq 0$.

(a) $v(\theta) \geq 0$. Otherwise $v(\psi(\theta)) = 3v(\theta)$, as $25\theta^3$ has strictly smaller valuation than the other three terms of $\psi(\theta)$, and $v(4\theta - 1) = v(\theta)$. Then (1.7) gives $8v(\theta) = v(\eta) + v(\theta)$, so $7v(\theta) = v(\eta) \geq 0$, a contradiction.

(b) $v(4\theta - 1) = 0$. Otherwise $\theta \equiv 1/4 \pmod{\mathfrak{P}}$, so θ is a unit and $\psi(\theta) \equiv \psi(1/4)$ is a unit. The left side of (1.7) is then a unit, while the right side has positive valuation.

(c) Hence $5v(\theta) + v(\psi(\theta)) = v(\eta)$, that is,

$$5v(\theta) + v(\theta - b) + v(\psi_1(\theta)) = v(\eta),$$

and the three terms on the left are ≥ 0, since θ, b and the coefficients of ψ_1 are $\mathfrak{P}$-integral.

(d) At most one of these three terms is positive. If $v(\theta) > 0$ then $\theta - b \equiv -b$ and $\psi(\theta) \equiv \psi(0) = 14$ are units, so $v(\theta - b) = v(\psi_1(\theta)) = 0$. If $v(\theta - b) > 0$ then $\theta \equiv b$ is a unit and $\psi_1(\theta) \equiv \psi_1(b)$ is a unit.

So $v(\theta - b)$ and $v(\psi(\theta)) = v(\theta - b) + v(\psi_1(\theta))$ both lie in $\{0, v(\eta)\} \subset 5\mathbb{Z}$. As $v(80000) = 0$, we get $v(E) = v(\theta - b) + 3v(\psi(\theta)) \equiv 0 \pmod 5$, and $v(E) = 0$ if moreover $p \nmid X$, because then $v(\eta) = 0$.

Case $p \mid Z$. Then $p \nmid X$, and $v(\eta) = -7em$ with $m = v_p(Z) \geq 1$.

(a) If $v(\theta) \geq 0$, the left side of (1.7) is integral, so $v(4\theta - 1) \geq 7em > 0$. Then $\theta \equiv 1/4$, so $\theta - b \equiv (1 - 4b)/4$ and $\psi(\theta) \equiv \psi(1/4)$ are units, and $v(E) = 0$.

(b) If $v(\theta) < 0$, then as before $v(\psi(\theta)) = 3v(\theta)$ and $v(4\theta - 1) = v(\theta)$, and (1.7) gives $7v(\theta) = v(\eta) = -7em$, so $v(\theta) = -em$. Then $v(\theta - b) = -em$ and $v(\psi(\theta)) = -3em$, so $v(E) = -10em \equiv 0 \pmod 5$.

This proves (ii) and (iii). The last assertion is (ii) applied to $K = L_{24}$. □

Proposition 3.2. *For every $\theta \in L_8$ with $\psi(\theta) \neq 0$,*

$$\mathrm{N}_{L_{24}/L_8}\Big(80000\,(\theta - b)\,\psi(\theta)^3\Big) = 2^{21} \cdot 5^{10} \cdot \psi(\theta)^{10} = 2 \cdot \big(2^4 \cdot 5^2 \cdot \psi(\theta)^2\big)^5.$$

In particular $\mathrm{N}_{L_{24}/L_8}(E) \equiv 2$ modulo $L_8^{\times 5}$.

Proof. By (2.1), $\mathrm{N}_{L_{24}/L_8}(\theta - b) = \psi(\theta)/25$, while $80000 = 2^7 \cdot 5^4$ and $\psi(\theta)$ lie in L_8, so their norms are their cubes. Hence the norm is $80000^3 \cdot (\psi(\theta)/25) \cdot \psi(\theta)^9 = 2^{21} \cdot 5^{10} \cdot \psi(\theta)^{10}$. □

Remark 3.3. In the notation of [23, §4.5.2] recalled in Section 1.5, put $w = 10\theta Z$. Then $g_1(w, Z) = w - 10bZ = 10Z(\theta - b)$ and $g(w, Z) = w^3 + 8w^2Z + 56wZ^2 + 560Z^3 = 40Z^3\psi(\theta)$, so

$$E = \frac{g_1(w, Z)\, g(w, Z)^3}{8Z^{10}}.$$

Here $80000 = 10 \cdot 40^3/8$, and the factor $1/8$ turns the power 2^{10} in $10 \cdot 40^3 = 2^{10} \cdot 5^4$ into the power 2^7 chosen in Section 1.4. The product $g_1 g^3$ is homogeneous of degree 10, so if $w = dw_0$ and $Z = dz_0$ with $d \in L_8^\times$, then modulo fifth powers E is $4\, g_1(w_0, z_0)\, g(w_0, z_0)^3$, that is, Putz's linear factor $g_1(w_0, z_0)$ multiplied by the element $4\, g(w_0, z_0)^3$ of L_8. Since $\mathrm{N}_{L_{24}/L_8}(g_1(w_0, z_0)) = g(w_0, z_0)$, the norm of $g_1(w_0, z_0)g(w_0, z_0)^3$ is $g(w_0, z_0)^{10}$, which is why the class of the norm of E does not depend on the solution.

4. The valuations of E at the primes above 2 and 5

At the prime of L_{24} above 2 the valuation of E modulo 5 follows from the norm identity (Lemma 4.1). At the seven primes above 5 the values are the same for every solution (Proposition 4.2) and give the condition (V) of Section 7. Without (V) the sieve does not eliminate every class (Remark 7.2(d)).

4.1. The prime above 2.

Lemma 4.1. *Let $\mathfrak{P}_1$ be the prime of L_{24} above 2. For every $\theta \in L_8$ with $\psi(\theta) \neq 0$,*

$$v_{\mathfrak{P}_1}\big(80000\,(\theta - b)\,\psi(\theta)^3\big) \equiv 3 \pmod 5.$$

Proof. As $\mathfrak{P}_1$ is the only prime of L_{24} above 2 and $f(\mathfrak{P}_1/2) = 1$, we have $v_{\mathfrak{P}_1}(\alpha) = v_2\big(\mathrm{N}_{L_{24}/\mathbb{Q}}(\alpha)\big)$ for $\alpha \in L_{24}^\times$. By Proposition 3.2,

$$\mathrm{N}_{L_{24}/\mathbb{Q}}(E) = \mathrm{N}_{L_8/\mathbb{Q}}\Big(2^{21} \cdot 5^{10} \cdot \psi(\theta)^{10}\Big) = 2^{168} \cdot 5^{80} \cdot \mathrm{N}_{L_8/\mathbb{Q}}(\psi(\theta))^{10},$$

so $v_{\mathfrak{P}_1}(E) = 168 + 10\, v_2\big(\mathrm{N}_{L_8/\mathbb{Q}}(\psi(\theta))\big) \equiv 168 \equiv 3 \pmod 5$. □

So the norm condition (N) of Section 7 already fixes the valuation at $\mathfrak{P}_1$ (Remark 7.2(a)).

4.2. **The primes above 5.** Recall from Lemmas 2.4, 2.5 and 2.6 the primes $\mathfrak{p}_A, \mathfrak{p}_B, \mathfrak{p}_C$ of L_8 above 5, with ramification indices 5, 1, 2, and the roots $b_1 \in \mathbb{Z}_5$ and b_2, b_3 of ψ over $\mathbb{Q}_5$. For a prime $\mathfrak{P}$ of L_{24} above 5 we have $v_{\mathfrak{P}}(\alpha) = e(\mathfrak{P}/5)\, v_5(\alpha)$, where α is viewed in the completion $L_{24,\mathfrak{P}}$ and v_5 is extended to it.

Proposition 4.2. *Let (X, Y, Z) be a solution with $A_\eta \simeq L_8$, and let θ and E be as in Section 3. Then $5 \nmid YZ$. Put $n = v_5(\eta) = 5v_5(X) \geq 0$. The valuations of E at the seven primes of L_{24} above 5 are*

label of $\mathfrak{P}$	$(1,1,1)$	$(2,1,1)$	$(5,1,5)$	$(10,1,5)$	$(2,1,2)$, *three primes*
$v_{\mathfrak{P}}(E)$	$4n+12$	$6n+18$	20	30	$6n+30,\ 8n+35,\ 6n+35$
$v_{\mathfrak{P}}(E) \bmod 5$	2	3	0	0	0, 0, 0

With the numbering of Table 2: $v_{\mathfrak{P}_3}(E) \equiv 2$, $v_{\mathfrak{P}_5}(E) \equiv 3$, and $v_{\mathfrak{P}_i}(E) \equiv 0 \pmod 5$ for $i \in \{2, 4, 6, 7, 8\}$.

The proof uses the hypothesis $A_\eta \simeq L_8$ only through the fact that θ generates L_8, so that

$$L_8 \otimes \mathbb{Q}_5 \simeq \mathbb{Q}_5[t]/(f_\eta), \qquad t \mapsto \theta. \tag{4.1}$$

The left side is the product of the three fields $L_{8,\mathfrak{p}_A}$, $L_{8,\mathfrak{p}_B} = \mathbb{Q}_5$, $L_{8,\mathfrak{p}_C}$, of degrees 5, 1, 2 and ramification indices 5, 1, 2. Under (4.1) the image $\theta_{\mathfrak{p}}$ of θ in $L_{8,\mathfrak{p}}$ generates $L_{8,\mathfrak{p}}$ and is a root of f_η. Its minimal polynomial over $\mathbb{Q}_5$ is an irreducible factor of f_η of degree $[L_{8,\mathfrak{p}} : \mathbb{Q}_5]$, and different primes give different factors. We write $\theta_A, \theta_B, \theta_C$ for the images of θ in $L_{8,\mathfrak{p}_A}, L_{8,\mathfrak{p}_B}, L_{8,\mathfrak{p}_C}$. From (1.7), since $v_5(4) = 0$, for $\bullet \in \{A, B, C\}$

$$v_5(\psi(\theta_\bullet)) = v_5(\eta) + v_5(4\theta_\bullet - 1) - 5v_5(\theta_\bullet), \qquad \psi(\theta_\bullet) = 25(\theta_\bullet - b_1)(\theta_\bullet - b_2)(\theta_\bullet - b_3). \tag{4.2}$$

Proof. Step 1: $5 \nmid Z$. Suppose $m = v_5(Z) \geq 1$, so $5 \nmid X$ and $v_5(\eta) = -7m$. The 5-adic valuations of the coefficients of $f_\eta = 100t^8 + 80t^7 + 56t^6 + 56t^5 - 4\eta t + \eta$ at $t^8, t^7, t^6, t^5, t^1, t^0$ are $2, 1, 0, 0, -7m, -7m$. The points $(5, 0)$, $(6, 0)$, $(7, 1)$ lie above the segment joining $(1, -7m)$ to $(8, 2)$, so the Newton polygon has vertices $(0, -7m)$, $(1, -7m)$, $(8, 2)$. The second segment has length 7 and slope $(7m + 2)/7$, whose denominator in lowest terms is 7. So $\mathbb{Q}_5[t]/(f_\eta)$ has a factor field whose ramification index is divisible by 7, whereas the factors of $L_8 \otimes \mathbb{Q}_5$ have ramification indices 5, 1, 2. This contradicts (4.1).

So $5 \nmid Z$ and $n = v_5(\eta) = 5v_5(X) \geq 0$. We now determine $\theta_A, \theta_B, \theta_C$.

Step 2: the case $n > 0$. The valuations of the coefficients are $2, 1, 0, 0$ at t^8, t^7, t^6, t^5 and n, n at t^1, t^0. The Newton polygon has vertices $(0, n)$, $(5, 0)$, $(6, 0)$, $(8, 2)$ (the point $(1, n)$ lies above the first segment and $(7, 1)$ lies on the last). So $f_\eta = g_A g_B g_C$ over $\mathbb{Q}_5$ with $\deg g_A = 5$, $\deg g_B = 1$, $\deg g_C = 2$, and the roots of g_A, g_B, g_C have valuations $n/5$, 0, -1. The algebra $\prod \mathbb{Q}_5[t]/(g_\bullet)$ has at least three factor fields, with equality only if every $g_\bullet$ is irreducible. By (4.1) it has exactly three, of degrees $5, 1, 2$. Hence θ_A, θ_B, θ_C are roots of g_A, g_B, g_C: $v_5(\theta_A) = n/5$, $\theta_B \in \mathbb{Z}_5^\times$, $v_5(\theta_C) = -1$.

Step 3: the case $n = 0$. Now η is a 5-adic unit. The Newton polygon has vertices $(0, 0)$, $(6, 0)$, $(8, 2)$: six unit roots and two roots of valuation -1. The two roots of valuation -1 form a factor of f_η of degree 2. By (4.1) the corresponding factor of $\mathbb{Q}_5[t]/(f_\eta)$ is a product of some of the fields $L_{8,\mathfrak{p}}$, so it is $L_{8,\mathfrak{p}_C}$, the only one of degree 2. So $v_5(\theta_C) = -1$, while $\theta_B \in \mathbb{Z}_5^\times$ and θ_A is a unit generating the totally ramified quintic field $L_{8,\mathfrak{p}_A}$. Modulo 5,

$$f_\eta \equiv t^6 + t^5 + \eta t + \eta = (t + 1)(t^5 + \eta) \equiv (t + 1)(t + \eta)^5,$$

so every unit root is congruent to -1 or to $-\eta$ modulo the maximal ideal.

For a unit root $\theta_\bullet \in \{\theta_A, \theta_B\}$ we have $v_5(\theta_\bullet - b_2) = v_5(\theta_\bullet - b_3) = -1$, so $v_5(\psi(\theta_\bullet)) = v_5(\theta_\bullet - b_1)$, and (4.2) gives $v_5(\psi(\theta_\bullet)) = v_5(4\theta_\bullet - 1)$. Hence

$$v_5(\theta_\bullet - b_1) = v_5(\psi(\theta_\bullet)) = v_5(\theta_\bullet - \tfrac{1}{4}) \qquad \text{for } \theta_\bullet \in \{\theta_A, \theta_B\} \text{ (when } n = 0). \tag{4.3}$$

Put $F(s) = f_\eta(\frac{1}{4} + s) = \sum_j c_j s^j$. Its roots are the numbers $\theta - \frac{1}{4}$ for the roots θ of f_η, and all c_j are 5-integral. The constant term $c_0 = f_\eta(\frac{1}{4}) = \psi(\frac{1}{4})/256 = 1225/16384$ has $v_5(c_0) = 2$, and

$$c_1 = f'_\eta(\tfrac{1}{4}) = \tfrac{823}{512} - 4\eta = -\tfrac{1225}{512} - 4(\eta - 1).$$

The product of the roots of F is $c_0/100$, of valuation 0, and the two roots coming from θ_C and its conjugate have valuation -1 each. So the valuations $v_5(\theta - \frac{1}{4})$ of the six unit roots add up to 2.

Step 4: $5 \nmid Y$. Suppose $5 \mid Y$. Then $n = 0$ and $v_5(1 - \eta) = v_5(Y^2/Z^7) = 2v_5(Y) \geq 2$. So $\eta \equiv 1 \pmod 5$, and all six unit roots are $\equiv -1 \equiv \frac{1}{4}$ modulo the maximal ideal. Thus $w_B = v_5(\theta_B - \frac{1}{4})$ is a positive integer ($\theta_B \neq \frac{1}{4}$ as $c_0 \neq 0$), and $w_A = v_5(\theta_A - \frac{1}{4})$, the same for the five conjugates of θ_A over $\mathbb{Q}_5$, is a positive element of $\frac{1}{5}\mathbb{Z}$ because $L_{8,\mathfrak{p}_A}$ has ramification index 5. From $w_B + 5w_A = 2$ we get $w_B = 1$ and $w_A = \frac{1}{5}$. So F has exactly one root of valuation 1 and no root of larger valuation, and the first segment of its Newton polygon joins $(0, 2)$ to $(1, 1)$, so $v_5(c_1) = 1$. But $v_5(1225) = 2$ and $v_5(\eta - 1) \geq 2$ give $v_5(c_1) \geq 2$. This contradiction shows $5 \nmid Y$.

Step 5: the case $n = 0$, continued. Now $5 \nmid XYZ$, so $\eta \not\equiv 0, 1 \pmod 5$. The factors $t + 1$ and $(t + \eta)^5$ are coprime modulo 5, so by Hensel's lemma the factor of f_η with the six unit roots is the product over $\mathbb{Q}_5$ of a linear factor with root $\equiv -1$ and a quintic factor with roots $\equiv -\eta$. Comparing degrees with $L_{8,\mathfrak{p}_B}$ and $L_{8,\mathfrak{p}_A}$, we get $\theta_B \equiv -1$ and $\theta_A \equiv -\eta$. Hence $\theta_A \not\equiv \frac{1}{4}$, that is, $v_5(\theta_A - \frac{1}{4}) = 0$. Also $v_5(c_1) = v_5(4(\eta - 1)) = 0$. The Newton polygon of F therefore begins with the segment from $(0, 2)$ to $(1, 0)$: exactly one root of F has positive valuation, and its valuation is 2. This root is $\theta_B - \frac{1}{4}$, so by (4.3)

$$v_5(\theta_B - b_1) = v_5(\psi(\theta_B)) = 2, \qquad v_5(\theta_A - b_1) = v_5(\psi(\theta_A)) = 0.$$

Step 6: the valuations of $\theta - b_i$ and $\psi(\theta)$. We show, for all $n \geq 0$:

(a) $v_5(\theta_A - b_1) = 0$, $v_5(\theta_A - b_2) = v_5(\theta_A - b_3) = -1$ and $v_5(\psi(\theta_A)) = 0$;
(b) $v_5(\theta_B - b_1) = v_5(\psi(\theta_B)) = n + 2$, and $v_5(\theta_B - b_2) = v_5(\theta_B - b_3) = -1$;
(c) $v_5(\theta_C - b_1) = -1$, $v_5(\psi(\theta_C)) = n + 4$, and $\{v_5(\theta_C - b_2), v_5(\theta_C - b_3)\} = \{n + \frac{3}{2}, \frac{3}{2}\}$.

For $n = 0$, (a) and the first part of (b) are Step 5. For $n > 0$: in (a), $v_5(\theta_A) = n/5 > 0$, so $\theta_A - b_1 \equiv -b_1$ is a unit and $\psi(\theta_A) \equiv 14$ is a unit. In (b), put $s = \theta_B - b_1$. By (4.2), $v_5(s) = v_5(\psi(\theta_B)) = n + v_5(4\theta_B - 1)$, where $4\theta_B - 1 = (4b_1 - 1) + 4s$ and $v_5(4b_1 - 1) = 2$. If $v_5(s) < 2$ then $v_5(4\theta_B - 1) = v_5(s)$ and $n = 0$. If $v_5(s) = 2$ then $v_5(4\theta_B - 1) \geq 2$ and $v_5(s) \geq n + 2 > 2$. Both are impossible, so $v_5(s) > 2$, $v_5(4\theta_B - 1) = 2$ and $v_5(s) = n + 2$. The remaining statements in (a) and (b) hold because θ_A, θ_B are integral and $v_5(b_2) = v_5(b_3) = -1$. In (c), for all $n \geq 0$: $v_5(\theta_C) = -1$ gives $v_5(4\theta_C - 1) = -1$ and $v_5(\theta_C - b_1) = -1$, so by (4.2) $v_5(\psi(\theta_C)) = n - 1 + 5 = n + 4$ and

$$v_5(\theta_C - b_2) + v_5(\theta_C - b_3) = n + 4 - 2 + 1 = n + 3.$$

Since $v_5(b_2 - b_3) = \frac{3}{2}$ (Lemma 2.6), if one of the two valuations exceeds $\frac{3}{2}$ the other equals $\frac{3}{2}$. If neither does, their sum is at most 3. For $n > 0$ this gives $\{n + \frac{3}{2}, \frac{3}{2}\}$. For $n = 0$ the sum is 3 and both equal $\frac{3}{2}$.

Step 7: the primes of L_{24} above 5. As in the proof of Lemma 2.5, each prime $\mathfrak{P}$ of L_{24} above 5 corresponds to a factor of $L_{8,\mathfrak{p}} \otimes (\mathbb{Q}_5 \times \mathbb{Q}_5(b_2))$ for $\mathfrak{p} \in \{\mathfrak{p}_A, \mathfrak{p}_B, \mathfrak{p}_C\}$, and in $L_{24,\mathfrak{P}}$ the elements θ and b map to $\theta_{\mathfrak{p}}$ and to b_1 (in the factor $L_{8,\mathfrak{p}} \otimes \mathbb{Q}_5$) or to b_2 or b_3 (in the other). By Lemma 2.5, $L_{8,\mathfrak{p}_C} \simeq \mathbb{Q}_5(b_2)$, so $L_{8,\mathfrak{p}_C} \otimes \mathbb{Q}_5(b_2)$ is a product of two copies of $L_{8,\mathfrak{p}_C}$, in which b maps to b_2 and to b_3 respectively. All three primes above $\mathfrak{p}_C$ have $e(\mathfrak{P}/5) = 2$. Using $v_{\mathfrak{P}}(E) = e(\mathfrak{P}/5)(v_5(80000) + v_5(\theta_{\mathfrak{p}} - b_i) + 3v_5(\psi(\theta_{\mathfrak{p}})))$, where b_i is the image of b in $L_{24,\mathfrak{P}}$, with $v_5(80000) = 4$, Step 6 gives:

- above $\mathfrak{p}_B$: at $(1,1,1)$, $b \mapsto b_1$ and $v_{\mathfrak{P}}(E) = 4 + (n+2) + 3(n+2) = 4n + 12$; at $(2,1,1)$, $b \mapsto b_2$ and $v_{\mathfrak{P}}(E) = 2\,(4 - 1 + 3(n+2)) = 6n + 18$;
- above $\mathfrak{p}_A$: at $(5,1,5)$, $b \mapsto b_1$ and $v_{\mathfrak{P}}(E) = 5 \cdot 4 = 20$; at $(10,1,5)$, $b \mapsto b_2$ and $v_{\mathfrak{P}}(E) = 10\,(4-1) = 30$;
- above $\mathfrak{p}_C$: with $b \mapsto b_1$, $v_{\mathfrak{P}}(E) = 2\,(4 - 1 + 3(n+4)) = 6n + 30$; with b mapped to a root $b_i \in \{b_2, b_3\}$ with $v_5(\theta_C - b_i) = n + \frac{3}{2}$, $v_{\mathfrak{P}}(E) = 2\,(4 + n + \frac{3}{2} + 3(n+4)) = 8n + 35$; with b mapped to the other one, $v_{\mathfrak{P}}(E) = 2\,(4 + \frac{3}{2} + 3(n+4)) = 6n + 35$.

Since $n = 5v_5(X) \equiv 0 \pmod 5$, the residues modulo 5 are as stated. □

Remark 4.3. The labels do not distinguish the three primes with label $(2,1,2)$, and the proof does not determine which of them carries which of the values $6n+30$, $8n+35$, $6n+35$. All three values are $\equiv 0 \pmod 5$, so condition (V) is the same for every assignment. Condition (V) concerns only the primes above 5: the valuations of E at the primes above 7 are left free.

5. Auxiliary primes

Here we derive the condition (Q) of Section 7. For sixteen primes $q \equiv 1 \pmod 5$, the splitting of L_8 at q shows that $q \nmid XYZ$ (Corollary 5.5). At such a prime the residue of θ at each prime of L_8 above q is a root of $f_{\bar\eta}$, where $\bar\eta = \eta \bmod q$. So the vector of fifth-power residue symbols of E at the primes of L_{24} above q lies in a finite set $I(q)$, which can be computed without knowing the solution (Proposition 5.3).

Throughout this section q is a prime, $q \notin \{2, 5, 7\}$. Then q is unramified in L_8 and in L_{24} (Lemma 2.4). For a prime $\mathfrak{q}$ of L_8 or $\mathfrak{Q}$ of L_{24} above q we write $k(\mathfrak{q})$, $k(\mathfrak{Q})$ for the residue fields and $f(\mathfrak{q}) = [k(\mathfrak{q}) : \mathbb{F}_q]$.

5.1. **Definitions.** The *type* of a nonzero polynomial over $\mathbb{F}_q$ is the multiset of the degrees of its irreducible factors, counted with multiplicity. The *type of L_8 at q* is the multiset $\{f(\mathfrak{q}) : \mathfrak{q} \mid q\}$. The *type* of an unramified étale $\mathbb{Q}_q$-algebra is the multiset of residue degrees of its factor fields. It is the multiset of orbit sizes of Frobenius on the roots of any defining polynomial. If a defining polynomial has coefficients in $\mathbb{Z}_q$, a unit leading coefficient and a separable reduction modulo q, this multiset is the type of that reduction.

For $q \equiv 1 \pmod 5$ let $\zeta_q \in \mathbb{F}_q$ be the $((q-1)/5)$-th power of the least positive primitive root modulo q. It is a primitive fifth root of unity in $\mathbb{F}_q$. For a prime $\mathfrak{Q}$ of L_{24} above q and a $\mathfrak{Q}$-unit α, the *fifth-power residue symbol* $\chi_{\mathfrak{Q}}(\alpha) \in \mathbb{F}_5$ is defined by

$$\alpha^{(\#k(\mathfrak{Q})-1)/5} \equiv \zeta_q^{\chi_{\mathfrak{Q}}(\alpha)} \pmod{\mathfrak{Q}}. \tag{5.1}$$

It is a homomorphism from the $\mathfrak{Q}$-units to $\mathbb{F}_5$ that vanishes on fifth powers. We use the same notation for an element $\bar\alpha \in k(\mathfrak{Q})^\times$. For a prime $\mathfrak{q}$ of L_8 above q the symbol $\chi_{\mathfrak{q}}$ is defined in the same way, with $k(\mathfrak{q})$ in place of $k(\mathfrak{Q})$.

Definition 5.1. Let $q \equiv 1 \pmod 5$. Call $\bar\eta \in \mathbb{F}_q \smallsetminus \{0, 1\}$ *admissible* if the type of $f_{\bar\eta}(t) = 4t^5\psi(t) - \bar\eta(4t-1) \in \mathbb{F}_q[t]$ is the type of L_8 at q. For admissible $\bar\eta$, an *admissible family* is a

choice, for each prime $\mathfrak{q}$ of L_8 above q, of a root $t_\mathfrak{q} \in k(\mathfrak{q})$ of $f_{\bar\eta}$ whose minimal polynomial over $\mathbb{F}_q$ has degree $f(\mathfrak{q})$, such that these minimal polynomials are pairwise distinct. Let $I(q) \subseteq \mathbb{F}_5^m$, where m is the number of primes $\mathfrak{Q}_1, \dots, \mathfrak{Q}_m$ of L_{24} above q, be the set of the vectors

$$\Big(\chi_{\mathfrak{Q}_k}\big(80000\,(t_{\mathfrak{q}_k} - \bar b)\,\psi(t_{\mathfrak{q}_k})^3\big)\Big)_{k=1}^{m}, \qquad \mathfrak{q}_k = \mathfrak{Q}_k \cap L_8,$$

over all admissible $\bar\eta$ and all admissible families. Here $\bar b$ is the residue of b modulo $\mathfrak{Q}_k$, and $t_{\mathfrak{q}_k}$ is viewed in $k(\mathfrak{Q}_k)$ through the inclusion $k(\mathfrak{q}_k) \subseteq k(\mathfrak{Q}_k)$ induced by $L_8 \subseteq L_{24}$.

The arguments of the symbols are nonzero: if t is a root of $f_{\bar\eta}$ with $\bar\eta \neq 0$ and $\psi(t) = 0$ then $\bar\eta(4t-1) = 0$, so $t = \frac14$. But $\psi(\frac14) = 5^2 \cdot 7^2/2^6 \neq 0$ in $\mathbb{F}_q$. So $\psi(t) \neq 0$, and in particular $t \neq \bar b$.

5.2. **The local algebras when q divides XYZ.** The next proposition is a version of [23, Proposition 4.11 and Table 4.12], proved here in the form used below.

Proposition 5.2. *Let (X, Y, Z) be a solution and $q \notin \{2, 5, 7\}$.*

(a) *If $q \mid X$, then $A_\eta \otimes \mathbb{Q}_q$ is unramified and its type is* $\mathrm{type}(\psi \bmod q) \cup \mathrm{type}(s^5 - c)$ *for some $c \in \mathbb{F}_q^\times$.*

(b) *If $q \mid Z$, then $A_\eta \otimes \mathbb{Q}_q$ is unramified and its type is* $\{1\} \cup \mathrm{type}(s^7 - c)$ *for some $c \in \mathbb{F}_q^\times$.*

(c) *Let Ψ_i run over the irreducible factors of $\Psi \bmod q$, let $d_i = \deg \Psi_i$, and let $r_i \in \mathbb{F}_{q^{d_i}}$ be a root of Ψ_i. If $q \mid Y$, then $A_\eta \otimes \mathbb{Q}_q$ is unramified, and there is $\alpha \in \mathbb{F}_q^\times$ such that its type is the union of the T_i, where $T_i = \{d_i, d_i\}$ if $\alpha(4r_i - 1)$ is a square in $\mathbb{F}_{q^{d_i}}$ and $T_i = \{2d_i\}$ otherwise.*

Proof. (a) Here $q \nmid Z$ and $v_q(\eta) = 5k$ with $k = v_q(X) \geq 1$. Write $\eta = q^{5k}\eta_0$ with $\eta_0 \in \mathbb{Z}_q^\times$. The coefficients of f_η have valuations 0 at t^8, t^7, t^6, t^5 and $5k$ at t^1, t^0, so the Newton polygon has vertices $(0, 5k)$, $(5, 0)$, $(8, 0)$, and $f_\eta = GH$ over $\mathbb{Q}_q$, where G has the five roots of valuation k and H the three unit roots. Since $f_\eta \equiv 4t^5\psi(t) \pmod q$ and $\psi(0) \neq 0$, the unit roots reduce to the roots of $\psi \bmod q$, which is separable of degree 3 ($\mathrm{disc}\,\psi = -2^2 \cdot 5^7 \cdot 7$, leading coefficient 25). So $\mathbb{Q}_q[t]/(H)$ is unramified of type $\mathrm{type}(\psi \bmod q)$. For G, the polynomial $F(s) = q^{-5k} f_\eta(q^k s) = 4s^5\psi(q^k s) - \eta_0(4q^k s - 1)$ has integral coefficients and $F \equiv 56s^5 + \eta_0 \pmod q$, which is separable of degree 5. So F has five integral roots, distinct modulo q; they are the roots of G divided by q^k. Hence $\mathbb{Q}_q[t]/(G)$ is unramified of type $\mathrm{type}(s^5 - c)$ with $c = -\eta_0/56 \bmod q$.

(b) Here $q \nmid X$ and $v_q(\eta) = -7k$ with $k = v_q(Z) \geq 1$. Write $\eta = q^{-7k}\eta_1$ with $\eta_1 \in \mathbb{Z}_q^\times$. Then

$$\Phi(t) = q^{8k} f_\eta(q^{-k}t) = 100t^8 + 80q^k t^7 + 56q^{2k}t^6 + 56q^{3k}t^5 - 4\eta_1 t + \eta_1 q^k \equiv 4t\,(25t^7 - \eta_1) \pmod q,$$

which is separable. As $\mathbb{Q}_q[t]/(f_\eta) \simeq \mathbb{Q}_q[t]/(\Phi)$, the algebra is unramified of type $\{1\} \cup \mathrm{type}(s^7 - c)$ with $c = \eta_1/25 \bmod q$.

(c) Here $v_q(\eta - 1) = v_q(-Y^2/Z^7) = 2k$ with $k = v_q(Y) \geq 1$. Write $\eta - 1 = q^{2k}\alpha$ with $\alpha \in \mathbb{Z}_q^\times$. By (1.3), $f_\eta = \Psi^2 - q^{2k}\alpha(4t - 1)$. The polynomial $\Psi \bmod q$ is separable of degree 4 ($\mathrm{disc}\,\Psi = -2^6 \cdot 5^2 \cdot 7^3$, leading coefficient 10), and $\Psi(\frac14) = -35/128 \neq 0$. Let $\tilde r$ be a root of Ψ in the maximal unramified extension W of $\mathbb{Q}_q$, with reduction r. In $F_r(s) = q^{-2k} f_\eta(\tilde r + q^k s)$ the coefficient of s^j is $q^{(j-2)k} f_\eta^{(j)}(\tilde r)/j!$: it is $-\alpha(4\tilde r - 1)$ for $j = 0$, $-4\alpha q^k$ for $j = 1$, $\Psi'(\tilde r)^2$ for $j = 2$, and divisible by q for $j \geq 3$. So $F_r \equiv \Psi'(r)^2 s^2 - \alpha(4r - 1) \pmod q$, a separable

quadratic. Its two roots lift to roots $s \in W$, and the eight numbers $\tilde{r} + q^k s$ (four $\tilde{r}$, two s each) are distinct roots of f_η, hence all of them. So the algebra is unramified, and Frobenius permutes the pairs $(r, \bar{s})$, where $\bar{s}$ is the reduction of s. If r is a root of the irreducible factor Ψ_i of Ψ mod q, the orbit of $(r, \bar{s})$ has size d_i if $\bar{s} \in \mathbb{F}_{q^{d_i}}$, that is, if $\alpha(4r-1)/\Psi'(r)^2$, equivalently $\alpha(4r-1)$, is a square in $\mathbb{F}_{q^{d_i}}$, and size $2d_i$ otherwise. □

5.3. **Primes not dividing XYZ.**

Proposition 5.3. *Let (X, Y, Z) be a solution with $A_\eta \simeq L_8$, and let θ and E be as in Section 3. Let $q \notin \{2, 5, 7\}$ with $q \nmid XYZ$, and $\bar{\eta} = \eta \bmod q$. Then $\bar{\eta} \notin \{0, 1\}$, the polynomial $f_{\bar{\eta}}$ is separable of degree 8 and its type is the type of L_8 at q. For each prime $\mathfrak{q}$ of L_8 above q, θ is $\mathfrak{q}$-integral, its residue $\bar{\theta}_\mathfrak{q} \in k(\mathfrak{q})$ is a root of $f_{\bar{\eta}}$ with minimal polynomial of degree $f(\mathfrak{q})$, and these minimal polynomials are pairwise distinct. The element E is a unit at every prime $\mathfrak{Q}$ of L_{24} above q, with*

$$E \equiv 80000\,(\bar{\theta}_\mathfrak{q} - \bar{b})\,\psi(\bar{\theta}_\mathfrak{q})^3 \pmod{\mathfrak{Q}}, \qquad \mathfrak{q} = \mathfrak{Q} \cap L_8.$$

Consequently, if also $q \equiv 1 \pmod 5$, then $\big(\chi_\mathfrak{Q}(E)\big)_{\mathfrak{Q}|q} \in I(q)$.

Proof. Since $q \nmid XYZ$ and $1 - \eta = Y^2/Z^7$, η is q-integral with $\bar{\eta} \neq 0, 1$. By Lemma 2.1, $f_{\bar{\eta}}$ is separable (its leading coefficient 100 is a unit). Then $f_\eta/100 \in \mathbb{Z}_q[t]$ is monic with unit discriminant, so $\mathbb{Z}_q[t]/(f_\eta)$ is étale over $\mathbb{Z}_q$ and is the maximal order of $\mathbb{Q}_q[t]/(f_\eta) \simeq L_8 \otimes \mathbb{Q}_q$ ($t \mapsto \theta$). Hence θ is integral at every $\mathfrak{q} \mid q$, and reduction gives an isomorphism $\mathbb{F}_q[t]/(f_{\bar{\eta}}) \simeq \prod_{\mathfrak{q}|q} k(\mathfrak{q})$, $t \mapsto (\bar{\theta}_\mathfrak{q})$. The left side is a product of fields, one for each irreducible factor of $f_{\bar{\eta}}$. An isomorphism between finite products of fields matches the factors bijectively. So each $\bar{\theta}_\mathfrak{q}$ is a root of exactly one irreducible factor of $f_{\bar{\eta}}$, which is its minimal polynomial and has degree $f(\mathfrak{q})$, and different primes $\mathfrak{q}$ give different factors. In particular the type of $f_{\bar{\eta}}$ is the type of L_8 at q. By Proposition 3.1(iii), E is a unit at every $\mathfrak{Q} \mid q$, and since the reductions of L_8 and L_{24} are compatible with $k(\mathfrak{q}) \subseteq k(\mathfrak{Q})$, E reduces to $80000(\bar{\theta}_\mathfrak{q} - \bar{b})\psi(\bar{\theta}_\mathfrak{q})^3$. So $\bar{\eta}$ is admissible and $(\bar{\theta}_\mathfrak{q})_\mathfrak{q}$ is an admissible family, which gives the last assertion. □

5.4. **The auxiliary primes.** We searched the primes $q \equiv 1 \pmod 5$ up to 700 for primes at which the splitting of L_8 excludes $q \mid XYZ$. Sixteen of them qualify, more than the sieve of Section 7 needs.

Proposition 5.4. *Among the primes $q \equiv 1 \pmod 5$ with $11 \le q \le 700$, the type of L_8 at q is not of any of the forms* (a), (b), (c) *of Proposition 5.2 (for any c, α) exactly for the sixteen primes*

$$q \in \mathcal{Q} = \{11, 101, 131, 181, 211, 251, 271, 311, 331, 401, 431, 461, 541, 601, 631, 661\}.$$

For these primes the types, the numbers of admissible residues $\bar{\eta}$, the numbers m of primes of L_{24} above q, and the sizes of the sets $I(q)$ are those of Table 3; the sets $I(q)$ are listed in Appendix A.5.

Proof. A finite computation (Appendix C): for each prime $q \equiv 1 \pmod 5$ up to 700, list all the types of the forms (a), (b), (c) over all $c, \alpha \in \mathbb{F}_q^\times$ and compare with the type of L_8 at q. For $q \in \mathcal{Q}$, enumerate the admissible $\bar{\eta}$ and families and compute the symbols. The type of L_8 at q is read off from the prime decomposition of q in L_8. For $q \in \mathcal{Q}$ the prime q does not divide the index $2^7 \cdot 5 \cdot 41$ of $\mathbb{Z}[a]$, so by the Dedekind–Kummer theorem it is also the type of h mod q. For $q = 41$, which divides the index, the type of L_8 at q is $\{1, 2, 5\}$, which is of the form (a). □

q	type of L_8	$\#\bar\eta$	m	$\#I(q)$	q	type of L_8	$\#\bar\eta$	m	$\#I(q)$
11	1,1,2,4	1	4	1	331	4,4	23	6	21
101	2,3,3	5	7	16	401	1,7	102	2	1
131	2,2,4	9	9	112	431	1,7	144	2	1
181	1,1,1,2,3	9	11	59	461	1,3,4	70	7	84
211	2,6	37	4	24	541	1,7	162	2	1
251	2,2,4	16	9	172	601	1,1,6	105	7	120
271	8	71	3	5	631	1,2,2,3	56	6	25
311	1,1,1,1,4	6	11	240	661	2,3,3	28	7	68

TABLE 3. The sixteen auxiliary primes: the type of L_8 at q, the number of admissible residues $\bar\eta \in \mathbb{F}_q$, the number m of primes of L_{24} above q, and the size of $I(q)$.

Corollary 5.5. *Let (X, Y, Z) be a solution with $A_\eta \simeq L_8$. For every $q \in \mathcal{Q}$ we have $q \nmid XYZ$ and $\big(\chi_{\mathfrak{Q}}(E)\big)_{\mathfrak{Q}|q} \in I(q)$.*

Proof. If $q \mid XYZ$, then by Proposition 5.2 the type of $A_\eta \simeq L_8$ at q would be of one of the forms (a), (b), (c), which Proposition 5.4 excludes. So $q \nmid XYZ$, and Proposition 5.3 applies. □

Remark 5.6. The single admissible residue at $q = 11$ is $\bar\eta = 7$, in agreement with [23, Theorem 4.34(v)].

6. THE GROUP $L_{24}(S, 5)$

The sieve of Section 7 is carried out in coordinates on $L_{24}(S, 5)$. Since the class number of L_{24} is 1, $L_{24}(S, 5)$ is the group of S-units of L_{24} modulo fifth powers, with an explicit basis (Proposition 6.2). The norm from L_{24} to L_8 is given by an explicit matrix (Lemma 6.3).

6.1. The class number of L_{24}.

Theorem 6.1. *The class number of L_{24} is 1.*

Appendix B proves it without assuming the generalized Riemann hypothesis. The descent uses only the consequence that 5 does not divide the class number of L_{24}, through Proposition 6.2(ii) below, and nothing about the class group of L_8.

6.2. A basis.

Let $\mathcal{O}_S$ be the ring of S-integers of L_{24}. If $\alpha \in L_{24}^\times$ represents a class in $L_{24}(S, 5)$, then $\alpha\,\mathcal{O}_S = \mathfrak{a}^5$ for a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_S$, and the class of $\mathfrak{a}$ in the class group $\mathrm{Cl}(\mathcal{O}_S)$ depends only on the class of α. This gives an exact sequence

$$0 \longrightarrow \mathcal{O}_S^\times/\mathcal{O}_S^{\times 5} \longrightarrow L_{24}(S, 5) \longrightarrow \mathrm{Cl}(\mathcal{O}_S)[5] \longrightarrow 0, \tag{6.1}$$

where the first map is injective because an S-unit that is a fifth power in L_{24} is the fifth power of an S-unit, and the kernel of the second consists of the classes of S-units: if $\mathfrak{a} = w\mathcal{O}_S$ then $\alpha w^{-5} \in \mathcal{O}_S^\times$. The second map is surjective: if $\mathfrak{a}^5 = \alpha\mathcal{O}_S$, then the class of α lies in $L_{24}(S, 5)$ and maps to that of $\mathfrak{a}$. The group $\mathrm{Cl}(\mathcal{O}_S)$ is a quotient of the class group of L_{24}. By Dirichlet's S-unit theorem, $\mathcal{O}_S^\times \simeq \mu(L_{24}) \times \mathbb{Z}^r$ with $r = r_1 + r_2 - 1 + \#S = 2 + 11 - 1 + 12 = 24$, and $\mu(L_{24}) = \{\pm 1\}$ because L_{24} has a real embedding. So $\mathcal{O}_S^\times/\mathcal{O}_S^{\times 5} \simeq \mathbb{F}_5^{24}$.

The elements $B_1, \dots, B_{24}$ of L_{24} are listed in Table 4, as polynomials in a and b. For $i \le 12$, B_i generates the prime $\mathfrak{P}_i$ of Table 2, and $B_{13}, \dots, B_{24}$ are units.

Proposition 6.2. (i) *The elements $B_1, \dots, B_{24}$ are S-units, $v_{\mathfrak{P}_i}(B_j) = 1$ if $i = j \le 12$ and $v_{\mathfrak{P}_i}(B_j) = 0$ otherwise, and their classes in $L_{24}^\times / L_{24}^{\times 5}$ are linearly independent over $\mathbb{F}_5$.*

(ii) *The classes of $B_1, \dots, B_{24}$ form a basis of $L_{24}(S,5) \simeq \mathbb{F}_5^{24}$.*

Proof. (i) Each B_j has a characteristic polynomial over $\mathbb{Q}$ whose coefficients have denominators divisible only by 2, 5 and 7, and its norm $\mathrm{N}_{L_{24}/\mathbb{Q}}(B_j)$ is -2 ($j=1$), 5 ($2 \le j \le 8$), -7 ($9 \le j \le 12$) or 1 ($j \ge 13$). So B_j is integral at every prime of L_{24} outside S, and its norm is prime to every rational prime other than 2, 5, 7. Hence B_j is an S-unit. The valuations are computed with `nfeltval`. For independence, let $\mathfrak{Q}$ run over the 97 primes of L_{24} above the sixteen primes of $\mathcal{Q}$. The 97×24 matrix $(\chi_{\mathfrak{Q}}(B_j))$ over $\mathbb{F}_5$ has rank 24 (the rows for $q \in \{11, 101, 131, 181\}$ already have rank 24). Each $\chi_{\mathfrak{Q}}$ is a homomorphism on the $\mathfrak{Q}$-units that vanishes on fifth powers. If $\prod_j B_j^{c_j} = \gamma^5$ with $\gamma \in L_{24}^\times$, then γ is an S-unit, hence a unit at every such $\mathfrak{Q}$, and applying the symbols gives $\sum_j c_j \chi_{\mathfrak{Q}}(B_j) = 0$ for all $\mathfrak{Q}$. As the matrix has rank 24, $c \equiv 0 \pmod 5$. These computations are listed in Appendix C.

(ii) Since $\mathrm{Cl}(\mathcal{O}_S)$ is a quotient of the class group of L_{24}, which is trivial by Theorem 6.1, we have $\mathrm{Cl}(\mathcal{O}_S)[5] = 0$ and (6.1) gives $L_{24}(S,5) = \mathcal{O}_S^\times / \mathcal{O}_S^{\times 5} \simeq \mathbb{F}_5^{24}$, in which the 24 independent classes of (i) form a basis. □

If the class of $\alpha \in L_{24}^\times$ lies in $L_{24}(S,5)$, we write $c = (c_1, \dots, c_{24}) \in \mathbb{F}_5^{24}$ for its coordinate vector on this basis. Since the valuation matrix $(v_{\mathfrak{P}_i}(B_j))_{i \le 12,\, j \le 24}$ is $(I_{12} \mid 0)$ by Proposition 6.2(i), $c_i \equiv v_{\mathfrak{P}_i}(\alpha) \pmod 5$ for $i \le 12$.

6.3. **The norm map.** Let $u_1, \dots, u_{10} \in L_8$ be the elements of Table 5: $u_1, \dots, u_6$ generate the primes of L_8 above 2, 5, 7 (the valuation matrix is the identity), and $u_7, \dots, u_{10}$ are units.

Lemma 6.3. (i) *The classes of $u_1, \dots, u_{10}$ in $L_8^\times / L_8^{\times 5}$ are linearly independent over $\mathbb{F}_5$.*

(ii) *There are exact identities*

$$\mathrm{N}_{L_{24}/L_8}(B_j) = \pm \prod_{i=1}^{10} u_i^{\mathsf{N}_{ij}} \quad (1 \le j \le 24), \qquad 2 = \pm \prod_{i=1}^{10} u_i^{\mathsf{T}_i},$$

with the integer matrix $\mathsf{N} \in M_{10\times 24}(\mathbb{Z})$ and vector $\mathsf{T} \in \mathbb{Z}^{10}$ printed in (A.1).

Proof. (i) The fifth-power residue symbols of $u_1, \dots, u_{10}$ at the 47 primes of L_8 above the primes of $\mathcal{Q}$ form a matrix of rank 10 over $\mathbb{F}_5$. Since the u_i are units at these primes, the argument of Proposition 6.2(i) shows that their classes are independent. This matrix can be recomputed from Tables 5 and 6: the primes of L_8 above q are the ideals $(q, h_k(a))$ of Table 6, with residue fields $\mathbb{F}_q[x]/(h_k)$.

(ii) For an element $B(a,b)$ of L_{24} written as a polynomial in a and b, $\mathrm{N}_{L_{24}/L_8}(B)$ is the resultant $\mathrm{Res}_t\left(\psi(t)/25,\, B(a,t)\right)$, computed exactly in $\mathbb{Q}[a]/(h(a))$. It equals the stated product up to sign, and the identity for 2 is checked by computing the product $\prod_i u_i^{\mathsf{T}_i}$ in the same ring. See Appendix C. □

7. The sieve, and the proof of Theorem 1.1

We now write the conditions of Sections 3, 4 and 5 in the coordinates of Section 6, show by a finite computation that no class satisfies all of them (Theorem 7.1), and deduce Theorem 1.1.

For each $q \in \mathcal{Q}$, number the primes of L_{24} above q as $\mathfrak{Q}_1, \dots, \mathfrak{Q}_m$ in the order of Appendix A.3, and let $M_q \in M_{m\times 24}(\mathbb{F}_5)$ be the matrix $\left(\chi_{\mathfrak{Q}_k}(B_j)\right)_{k,j}$, printed in Appendix A.4. The sets $I(q) \subseteq \mathbb{F}_5^m$ of Definition 5.1, with coordinates in the same order, are printed in Appendix A.5.

Theorem 7.1. *There is no $c \in \mathbb{F}_5^{24}$ satisfying all of the following conditions:*

(N) $\mathsf{N}c \equiv \mathsf{T} \pmod 5$*;*

(V) $c_3 = 2$*,* $c_5 = 3$ *and* $c_2 = c_4 = c_6 = c_7 = c_8 = 0$*;*

(Q) $M_q c \in I(q)$ *for* $q = 181, 311, 131, 251, 101$*.*

More precisely, the matrix N *has rank* 10 *over* $\mathbb{F}_5$*, so* (N) *defines an affine subspace of* $\mathbb{F}_5^{24}$ *of dimension* 14*; adding* (V) *gives an affine subspace* $\mathcal{A}$ *of dimension* 10*, that is,* $5^{10} = 9\,765\,625$ *vectors. Imposing* (Q) *for* $q = 181, 311, 131, 251, 101$ *in turn leaves* 36 875*,* 567*,* 19*,* 1 *and* 0 *vectors.*

Proof. Of the seven conditions in (V), only four are independent of (N). Indeed, the rows of (N) for the three primes of L_8 above 5, generated by u_2, u_3 and u_4, say that the norm has valuation 0 modulo 5 there; since every prime of L_{24} above 5 has residue degree 1 over L_8, these rows read $c_6 + c_7 \equiv 0$, $c_3 + c_5 \equiv 0$ and $c_2 + c_4 + c_8 \equiv 0$, and (V) satisfies them. The affine space $\mathcal{A}$ is $\{c_0 + \sum_{k=1}^{10} \lambda_k d_k : \lambda \in \mathbb{F}_5^{10}\}$ with c_0 and $d_1, \dots, d_{10}$ printed in (A.2). All 5^{10} of its elements were listed and tested against (Q) by arithmetic modulo 5 (Appendix C). The 19 vectors that satisfy (Q) for $q = 181, 311, 131$ are printed in Table 8 together with their images under M_{251}. Exactly one of these images lies in $I(251)$, and for that vector c^*,

$$M_{101}\, c^* = (1, 4, 2, 3, 0, 3, 0) \notin I(101),$$

by the list of $I(101)$ in Appendix A.5. □

Each count is the number of classes of $L_{24}(S, 5)$ satisfying the conditions imposed so far, so it does not depend on the basis $B_1, \dots, B_{24}$ or on the elements u_i. The intermediate counts depend on the order in which the five primes are imposed, but the final count does not. The five primes are those with the smallest proportion $\#I(q)/5^m$ (Table 3), taken in increasing order of that proportion. A separately written program gives the same counts (Appendix C.2).

Proof of Theorem 1.1. Suppose that (X, Y, Z) is a solution with $A_\eta \simeq L_8$. Let $\theta \in L_8$ and E be as in Section 3.

(1) By Proposition 3.1, the class of E lies in $L_{24}(S, 5)$. By Proposition 6.2(ii) it has a coordinate vector $c \in \mathbb{F}_5^{24}$: $E = \beta^5 \prod_j B_j^{c_j}$ with $\beta \in L_{24}^\times$ and integers c_j (read modulo 5).

(2) Condition (N). By Proposition 3.2, $\mathrm{N}_{L_{24}/L_8}(E) \in 2\, L_8^{\times 5}$. Taking norms in (1) and using Lemma 6.3(ii), $\prod_i u_i^{(\mathsf{N}c - \mathsf{T})_i} \in \pm L_8^{\times 5} = L_8^{\times 5}$, so $\mathsf{N}c \equiv \mathsf{T} \pmod 5$ by Lemma 6.3(i).

(3) Condition (V). For $\mathfrak{P} \in S$ we have $v_\mathfrak{P}(E) = 5v_\mathfrak{P}(\beta) + \sum_j c_j v_\mathfrak{P}(B_j)$, so $c_i \equiv v_{\mathfrak{P}_i}(E) \pmod 5$ for $i \le 12$. By Proposition 4.2 and Table 2, $v_{\mathfrak{P}_3}(E) \equiv 2$, $v_{\mathfrak{P}_5}(E) \equiv 3$ and $v_{\mathfrak{P}_i}(E) \equiv 0$ for $i \in \{2, 4, 6, 7, 8\}$.

(4) Condition (Q). Let $q \in \mathcal{Q}$. By Corollary 5.5, $q \nmid XYZ$ and $\left(\chi_{\mathfrak{Q}_k}(E)\right)_k \in I(q)$. By Proposition 3.1(iii) and since the B_j are S-units, E and the B_j are units at every $\mathfrak{Q}_k$, hence so is β, and $\chi_{\mathfrak{Q}_k}(E) = \sum_j c_j \chi_{\mathfrak{Q}_k}(B_j)$. So $M_q c \in I(q)$.

This contradicts Theorem 7.1. □

Remark 7.2. The following computations lie outside the proof. They show how much each condition contributes (Appendix C).

(a) On the affine space defined by (N), the first coordinate, which is the valuation at $\mathfrak{P}_1$ modulo 5, is identically 3, in agreement with Lemma 4.1.

(b) With all sixteen primes of $\mathcal{Q}$ imposed, no vector survives. If any single prime of $\mathcal{Q}$ is omitted, still none survives, except that 2, 2 and 1 vectors survive when 131, 181 or 311, respectively, is omitted.

(c) For each of the five primes $q = 181, 311, 131, 251, 101$, every vector of $I(q)$ is attained as $M_q c$ with $c \in \mathcal{A}$, so no element of $I(q)$ is excluded by (N) and (V) alone.

(d) If the values 2 and 3 that (V) prescribes at $\mathfrak{P}_3$ and $\mathfrak{P}_5$ are exchanged, again no vector survives, so the conclusion does not depend on telling these two primes apart. Without condition (V), exactly 6 vectors satisfy (N) and (Q) for all sixteen primes, and none of them satisfies (V).

Remark 7.3. Five primes can be expected to suffice for the following reason. Let $q \in \mathcal{Q}$, let $\mathfrak{q}$ be a prime of L_8 above q, and let $\alpha \in L_{24}$ be a unit at every prime above $\mathfrak{q}$. Since $\chi_{\mathfrak{Q}}(\alpha) = \chi_{\mathfrak{q}}(\mathrm{N}_{k(\mathfrak{Q})/k(\mathfrak{q})}\,\bar{\alpha})$ for $\mathfrak{Q} \mid \mathfrak{q}$, and q is unramified in L_{24},

$$\sum_{\mathfrak{Q}\mid\mathfrak{q}} \chi_{\mathfrak{Q}}(\alpha) = \chi_{\mathfrak{q}}(\,\mathrm{N}_{L_{24}/L_8}(\alpha)\,).$$

On $\mathcal{A}$ the norm class is that of 2, by (N). So for $c \in \mathcal{A}$ the symbols of $\prod_j B_j^{c_j}$ above each prime $\mathfrak{q}$ add up to $\chi_{\mathfrak{q}}(2)$, and $c \mapsto M_q c$ takes at most $5^{m-m'}$ values on $\mathcal{A}$, where m' is the number of primes of L_8 above q. When $m' = m$, as for $q = 11$, 401, 431 and 541, it takes a single value, which lies in $I(q)$, so the condition at q gives no information, although $\#I(q) = 1$ there. For the five primes of Theorem 7.1 it takes exactly $5^{m-m'}$ values, and by Remark 7.2(c) every element of $I(q)$ is one of them. The fractions of these values that lie in $I(q)$ are

$$\frac{59}{5^6}, \qquad \frac{240}{5^6}, \qquad \frac{112}{5^6}, \qquad \frac{172}{5^6}, \qquad \frac{16}{5^4}$$

for $q = 181$, 311, 131, 251, 101. In particular the condition at 181 keeps $59 \cdot 5^4 = 36\,875$ of the 5^{10} vectors of $\mathcal{A}$, as in Theorem 7.1. If the five conditions were independent, the expected number of surviving vectors would be $5^{10} \cdot 59 \cdot 240 \cdot 112 \cdot 172 \cdot 16/5^{28} \approx 0.001$.

8. A test on fibres where the descent element exists

A sieve that ends with no survivors could in principle do so because a condition was implemented wrongly. To test the implementation, we applied the same programs to fibres of φ above rational points of a twisted equation, where the element E is defined and its class must survive every condition. Propositions 3.1 and 3.2 use only coprime nonzero integers X, Z and a root θ of f_η, not a solution of (1.1), so they apply to such fibres (for Proposition 3.2 because ψ is irreducible over any field of degree 8, as in Lemma 2.4(c)). We use the twisted equation

$$X^5 + 2Y^2 = Z^7,$$

because the fibres above its points with X, Z coprime and $Y \neq 0$ are, like L_8, unramified outside 2, 5 and 7 (the arguments of Propositions 5.2 and 5.3 apply). It has the points $(X, Y, Z) = (-1, 1, 1)$ and $(-3, 11, -1)$, which give $\eta = X^5/Z^7 = -1$ and $\eta = 243$. For each of them, let $K_8 = A_\eta$ and $K_{24} = K_8(b)$.

- In both cases f_η is irreducible with Galois group S_8, and K_8 is an octic field of signature $(2, 3)$ and discriminant $-2^{18} \cdot 5^6 \cdot 7^7$, not isomorphic to L_8. The field K_{24} has degree 24, signature $(2, 11)$ and discriminant $-2^{56} \cdot 5^{20} \cdot 7^{23}$, and eleven primes above 2, 5 and 7: one above 2, six above 5 and four above 7. Its class number, computed assuming the generalized Riemann hypothesis, is 2 for $\eta = -1$ and 1 for $\eta = 243$. Let S now be the set of these eleven primes. In both cases the class number is prime to 5, so, under the same hypothesis, $K_{24}(S, 5)$ has dimension 23, the rank of the S-units of K_{24}. These class numbers are used only in this test.
- Let $\theta \in K_8$ be the class of t and $E = 80000(\theta - b)\psi(\theta)^3 \in K_{24}$. Its valuations at the primes outside S are divisible by 5: for $\eta = -1$ it is an S-unit, and for $\eta = 243$ (where $3 \mid X$) it has three prime factors above 3, with exponents 20, 15 and 15. Its coordinate vector c_E on a basis of $K_{24}(S, 5)$ satisfies the norm condition, formed as (N) is in Section 7 but with this basis and with S-units of K_8.
- At the six primes of K_{24} above 5, the valuations of E modulo 5 are 2 at the prime with label $(1, 1, 1)$, 3 at the prime with label $(2, 1, 1)$ and 0 at the other four, and its valuation at the prime above 2 is $\equiv 3$: the values that Lemma 4.1 and Proposition 4.2 give in the case $5 \nmid XYZ$. We impose these valuations at the primes above 5 in place of (V). Together with the norm condition they define an affine subspace of dimension 10.
- For the first twelve primes $q \equiv 1 \pmod 5$ not dividing XYZ, the set $I_{K_8}(q)$, defined as in Definition 5.1 with K_8 in place of L_8, contains the vector of residue symbols of E, and this vector equals $M_q c_E$, where M_q now denotes the matrix of residue symbols of the basis of $K_{24}(S, 5)$.
- The sieve with the norm condition, these valuations and the twelve primes leaves exactly one of the 5^{10} classes of this affine subspace, and it is c_E. With the primes taken in increasing order of $\#I_{K_8}(q)/5^m$, as in Section 7, one class remains after five primes for $\eta = -1$ (the counts are 350, 31, 3, 2, 1) and after six primes for $\eta = 243$ (the counts are 30 000, 30 000, 514, 40, 9, 1).

Appendix A. The data of the sieve

This appendix prints the data of the sieve: the basis of $L_{24}(S, 5)$, the elements u_i and the norm matrix, the primes of L_{24} above the auxiliary primes, the symbol matrices M_q, the sets $I(q)$, the affine space $\mathcal{A}$ of Theorem 7.1 and the last stages of the sieve. The same data, in machine-readable form, are part of the deposited programs and data [14], and the tables below are generated from them. Throughout, a is a root of h and b a root of ψ, as in Section 2.2.

A.1. **The basis of $L_{24}(S, 5)$.** Table 4 lists $B_1, \dots, B_{24}$. Any other elements with the same classes modulo $L_{24}^{\times 5}$ would serve equally well. All B_j are algebraic integers, since their valuations are nonnegative at every prime. The denominators D_j appear because the ring of integers of L_{24} is not contained in $\mathbb{Z}[a, b]$ (41 divides the index of $\mathbb{Z}[a]$ in the ring of integers of L_8, and L_8 and $\mathbb{Q}(b)$ are both ramified at 2, 5 and 7).

TABLE 4. The basis $B_1, \ldots, B_{24}$ of $L_{24}(S,5)$: $B_j = D_j^{-1} \sum_{k=0}^{2} \sum_{i=0}^{7} n_{j,k,i}\, a^i b^k$, with the coefficient vectors $(n_{j,k,0}, \ldots, n_{j,k,7})$ listed for $k = 0, 1, 2$. For $j \le 12$, $B_j \mathcal{O}_{L_{24}} = \mathfrak{P}_j$ (Table 2); $B_{13}, \ldots, B_{24}$ are units.

j	D_j	k	$(n_{j,k,0}, \ldots, n_{j,k,7})$
1	57400	0	(616000, 2248260, 891800, −1045688, −793184, −129318, 19824, 5096)
		1	(547500, −315440, −816200, −218468, 70426, 25772, −1356, −564)
		2	(−4185000, −2994100, 1328250, 1522730, 283140, −45170, −11215, 415)
2	57400	0	(−9240840, 74060, 8339100, 1141420, −2039352, −586194, 41202, 18214)
		1	(22069160, −2441640, −18373100, −1773180, 4462728, 1205316, −92178, −37796)
		2	(36027400, −2682100, −30642750, −3512700, 7422420, 2093490, −149295, −65690)
3	57400	0	(1140160, 386680, −1017520, −456624, 233212, 136276, 616, −4732)
		1	(2379260, 205380, −2220620, −502664, 559582, 201446, −9734, −6312)
		2	(6561400, 228200, −5753050, −1138210, 1398480, 478940, −21635, −15555)
4	28700	0	(23989086072840, 30139833484950, 990502126600, −13649681055976, −6676750244206, −713037035417, 181683706414, 34086470894)
		1	(9523819929090, 13514680552400, 3428310034850, −3221358499136, −1987091283791, −247661314582, 50989168649, 10401811379)
		2	(−19950643879900, −23312801675250, 2611366226500, 13839146593710, 6303844887010, 633088295145, −175025073765, −31891577190)
5	28700	0	(−985991160, −1214681790, 45500, 586244540, 280715946, 29402093, −7682248, −1426950)
		1	(−987651460, −1269154590, −98832550, 518104290, 261059956, 28510293, −7045973, −1336395)
		2	(138646850, 120698650, −105762000, −164166900, −65775785, −5836355, 1900530, 329450)
6	57400	0	(−3409000, 866180, 3970960, −94976, −1306928, −153398, 65884, −728)
		1	(−22996300, −3982520, 20509460, 5247264, −4916358, −1654828, 92074, 50142)
		2	(12363000, 2897200, −14398100, −5760290, 4181880, 2306080, 11860, −83745)
7	57400	0	(768600, 1877540, −56280, −1211448, −330120, 71890, 19068, −2716)
		1	(−1450000, −348260, 1207520, 329672, −200520, −77430, 2268, 2444)
		2	(−115000, 2968600, 826550, −1841420, −687800, 92300, 34895, −3840)
8	57400	0	(77409080, −21088200, −54959380, −47376, 12798408, 2755340, −286874, −87668)
		1	(−594422120, 19859600, 522388420, 69547264, −127339012, −37057640, 2529766, 1158932)
		2	(−774131800, 49629000, 663727550, 79007210, −161013680, −45581100, 3242865, 1427105)
9	57400	0	(−108290280, −116689020, 12816300, 58431212, 24139640, 2147194, −669410, −118398)
		1	(−145634980, −140864820, 29101200, 66358132, 18644890, −327706, −588520, −40488)
		2	(−28757200, −9864800, 18855500, 566730, −10390400, −3287840, 202700, 111055)
10	57400	0	(113032920, −10160640, −95216800, −10227644, 23020088, 6410796, −442456, −195678)
		1	(17117420, −8368840, −10121100, 1822816, 2312718, 243396, −64106, −8998)
		2	(−125798700, 3544900, 110694750, 14902740, −27007730, −7811310, 577535, 252530)
11	57400	0	(7091450800, 9293229960, 1045060100, −3489201268, −1808229444, −201743192, 48451410, 9289574)
		1	(−9223554500, −10462728340, 1824257600, 6844205352, 3048835666, 299804258, −85204360, −15377006)
		2	(−19516815000, −23744790100, 719652750, 12213711280, 5768619240, 598529870, −158503025, −29331340)

j	D_j	k	$(n_{j,k,0}, \ldots, n_{j,k,7})$
12	57400	0	(2634800, 80220, −3025260, −583968, 986580, 344078, −17682, −11088)
		1	(−5200, 1063820, 905840, −259848, −401220, −81602, 10108, 2742)
		2	(7942000, 3017300, −6039900, −2612970, 1134200, 563470, −12880, −16995)
13	5	0	(−1, 0, 0, 0, 0, 0, 0, 0)
		1	(9, 0, 0, 0, 0, 0, 0, 0)
		2	(10, 0, 0, 0, 0, 0, 0, 0)
14	28700	0	(5349820, −284270, −4457390, −511644, 1076124, 300167, −21987, −9366)
		1	(4679370, −259570, −3891390, −476234, 919389, 258167, −18787, −8006)
		2	(5980550, −671050, −4929600, −393010, 1234085, 327005, −25680, −10340)
15	28700	0	(−19068560, −14470260, 5720470, 8143184, 2262386, −11984, −72835, −5950)
		1	(−8892210, −19736860, −7953330, 7518324, 6174471, 1045676, −153485, −40175)
		2	(14361850, −3765400, −16321200, −1955640, 4070065, 1196390, −79900, −37750)
16	57400	0	(45994480, −269640, −40799640, −6129536, 9940084, 3017840, −191828, −94528)
		1	(52616480, 2206260, −47836240, −7983896, 11513624, 3585770, −218488, −111988)
		2	(−22420300, 5286400, 17270150, 716060, −4329890, −1068700, 93305, 33930)
17	57400	0	(2158520, −821100, −2342480, 81088, 547344, 34370, −18144, −364)
		1	(−2326980, −1932100, 1023820, 1185368, 194834, −35510, −7154, 176)
		2	(7525300, 1056000, −5388950, −1112980, 774510, 104100, −24185, −1110)
18	57400	0	(−160876800, −30380000, 153956180, 44774156, −39381076, −15244124, 648886, 474194)
		1	(−234186200, −20546800, 221268680, 45660216, −56727736, −17659084, 1154116, 535054)
		2	(−57100500, 15280500, 51725200, −5732510, −13395290, −371510, 466740, −4565)
19	28700	0	(238840, 22330, −84490, 28042, −6594, −8911, 217, 329)
		1	(365940, 141230, −338690, −139238, 84016, 37829, −1013, −1106)
		2	(524100, 113450, −172850, 18680, −31760, −26065, 55, 910)
20	28700	0	(−106159200, 3958500, 92800120, 12297096, −22584198, −6573112, 448252, 205632)
		1	(−245610250, 16403850, 210156070, 24861656, −50992253, −14425687, 1027127, 451782)
		2	(−142733750, 13286500, 119686050, 12641590, −28964045, −7988430, 590655, 250480)
21	57400	0	(−2887080, 2290120, 2927120, −544936, −979944, −232792, 19628, 8428)
		1	(3742120, −579380, −3344880, −142796, 857716, 187378, −20132, −5682)
		2	(−12868200, 2909300, 12643050, 580060, −3631260, −931330, 78645, 29770)
22	57400	0	(−429240, −500640, 726460, 577276, −227864, −188300, −1862, 6398)
		1	(3351660, 1741360, −3100240, −1612764, 728446, 393520, −7452, −12142)
		2	(3307400, −1224600, −2024850, 411540, 348440, −21200, −11905, 870)
23	28700	0	(1772260, 2311750, 25760, −1158528, −569296, −61929, 15526, 2968)
		1	(8954310, 10412450, −320440, −4957708, −2260331, −221849, 62166, 11228)
		2	(7593400, 8823000, −182850, −4090870, −1866090, −180860, 51615, 9170)
24	57400	0	(−14283360, −13039040, 1359120, 5240536, 1860628, 79772, −56896, −6272)
		1	(−5585460, 22055160, 15348820, −10889104, −9750142, −1555348, 255734, 57398)
		2	(11948100, 41679900, 15658550, −19039810, −13428130, −1865470, 362385, 73095)

A.2. **The norm data.** Table 5 lists $u_1, \ldots, u_{10} \in L_8$, and (A.1) gives the matrix N and the vector T of Lemma 6.3: column j of N is the exponent vector of $\mathrm{N}_{L_{24}/L_8}(B_j)$ on $u_1, \ldots, u_{10}$, up to sign, and T is that of 2.

i	D_i	$(n_{i,0},\dots,n_{i,7})$
1	820	(−11240, −3930, 11410, 4970, −2840, −1577, −13, 57)
2	820	(144740, 4910, −112770, −20720, 23320, 7193, −443, −218)
3	410	(−151490, −13740, 114790, 24900, −22370, −7289, 414, 219)
4	820	(1109580, −63670, −958820, −114980, 233100, 65447, −4742, −2042)
5	164	(428604, −30740, −362830, −41928, 87380, 24500, −1771, −766)
6	820	(17800, 17460, −14690, −9890, 2430, 1782, 13, −57)
7	410	(−1773690, 126310, 1512960, 175320, −366800, −103292, 7397, 3237)
8	820	(−44757080, 5683670, 36575370, 3213340, −8812930, −2344379, 182619, 73674)
9	820	(−49340, 25970, 28570, −7990, −5860, 363, 257, −23)
10	205	(−744505, −1104185, 1381795, 632240, −360460, −164188, 5128, 5033)

TABLE 5. The elements $u_i = D_i^{-1}\sum_{k=0}^{7} n_{i,k}a^k$ of L_8. The elements $u_1,\dots,u_6$ generate the primes of L_8 above 2, 5, 5, 5, 7, 7 with ramification indices 8, 5, 1, 2, 1, 7; $u_7,\dots,u_{10}$ are units.

$$\mathsf{N} = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&-3&-1&0&0&0&0&1&-1&0&0&0&0&0&-1&0&0&1&1&2&-1&0&0&0&0&0&0&0&0\\
0&0&-1&1&0&-1&0&0&-1&-1&0&-1&0&0&0&0&0&-1&0&0&0&-1&1&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&1&0&0&-1&0&0&0&1&0&1&0&1&-1&0&-1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&-1&-1&0&0&0&0&0&0&0&0
\end{pmatrix}, \qquad \mathsf{T} = \begin{pmatrix} 8\\0\\0\\0\\0\\0\\-1\\-1\\1\\3 \end{pmatrix}. \tag{A.1}$$

A.3. **The primes above the auxiliary primes.** Table 6 describes the primes $\mathfrak{O}_1,\dots,\mathfrak{O}_m$ of L_{24} above each $q \in \mathcal{Q}$ by their residue maps. Since $q \nmid 2\cdot 5\cdot 7\cdot 41$, the prime $\mathfrak{q} = \mathfrak{O}\cap L_8$ is $(q, h_k(a))$ for an irreducible factor h_k of $h \bmod q$ (the Dedekind–Kummer theorem), b is $\mathfrak{O}$-integral, and the primes of L_{24} above $\mathfrak{q}$ correspond to the irreducible factors of ψ over $k(\mathfrak{q})$. To compute $\chi_{\mathfrak{O}_k}(B_j)$ from the table, reduce the coefficients of B_j modulo q (they are q-integral), map a to x in $\mathbb{F}_q[x]/(h_k)$ and b to $r(x)$, or, in the rows marked "cubic" or "quadratic", to a root of that factor of ψ over $\mathbb{F}_q[x]/(h_k)$, and apply (5.1). The symbol does not depend on which root is chosen.

TABLE 6. The primes $\mathfrak{O}_1,\dots,\mathfrak{O}_m$ of L_{24} above the auxiliary primes q, in the order used for M_q and $I(q)$. The prime $\mathfrak{q}_k = \mathfrak{O}_k \cap L_8$ is $(q, h_k(a))$, and $k(\mathfrak{q}_k) = \mathbb{F}_q[x]/(h_k)$ with $a \mapsto x$. The last column gives the residue of b: either $b \equiv r(a) \pmod{\mathfrak{O}_k}$ with $r \in \mathbb{F}_q[x]$ (then $f(\mathfrak{O}_k) = \deg h_k$); or "cubic", when ψ is irreducible over $k(\mathfrak{q}_k)$ and $\mathfrak{O}_k = \mathfrak{q}_k\mathcal{O}_{L_{24}}$; or "quadratic", when ψ has one root in $k(\mathfrak{q}_k)$ and $\mathfrak{O}_k$ is the prime above $\mathfrak{q}_k$ at which b reduces to a root of the quadratic factor. The column ζ_q gives the fifth root of unity of (5.1).

q	ζ_q	k	$f(\mathfrak{O}_k)$	h_k	residue of b
11	4	1	3	$x+7$	cubic
		2	3	$x+6$	cubic
		3	6	x^2+3x+9	cubic
		4	12	$x^4+10x^3+8x^2+2x+7$	cubic
101	95	1	2	$x^2+46x+64$	$b \equiv 70a+3$
		2	2	$x^2+46x+64$	$b \equiv 62$
		3	2	$x^2+46x+64$	$b \equiv 31a+15$
		4	3	$x^3+54x^2+85x+97$	$b \equiv 62$

q	ζ_q	k	$f(\mathfrak{Q}_k)$	h_k	residue of b
		5	3	$x^3 + 5x^2 + 71x + 81$	$b \equiv 62$
		6	6	$x^3 + 5x^2 + 71x + 81$	quadratic
		7	6	$x^3 + 54x^2 + 85x + 97$	quadratic
131	53	1	2	$x^2 + 23x + 77$	$b \equiv 56a + 62$
		2	2	$x^2 + 41x + 41$	$b \equiv 126a + 36$
		3	2	$x^2 + 23x + 77$	$b \equiv 75a + 84$
		4	2	$x^2 + 41x + 41$	$b \equiv 5a + 110$
		5	2	$x^2 + 23x + 77$	$b \equiv 89$
		6	2	$x^2 + 41x + 41$	$b \equiv 89$
		7	4	$x^4 + 71x^3 + 49x + 99$	$b \equiv 89$
		8	4	$x^4 + 71x^3 + 49x + 99$	$b \equiv 31a^3 + 41a^2 + 96a + 27$
		9	4	$x^4 + 71x^3 + 49x + 99$	$b \equiv 100a^3 + 90a^2 + 35a + 119$
181	59	1	1	$x + 95$	$b \equiv 141$
		2	1	$x + 69$	$b \equiv 141$
		3	1	$x + 66$	$b \equiv 141$
		4	2	$x + 95$	quadratic
		5	2	$x^2 + 177x + 168$	$b \equiv 142a + 170$
		6	2	$x^2 + 177x + 168$	$b \equiv 141$
		7	2	$x + 69$	quadratic
		8	2	$x + 66$	quadratic
		9	2	$x^2 + 177x + 168$	$b \equiv 39a + 14$
		10	3	$x^3 + 140x^2 + 32x + 148$	$b \equiv 141$
		11	6	$x^3 + 140x^2 + 32x + 148$	quadratic
211	107	1	6	$x^6+175x^5+47x^4+39x^3+188x^2+151x+31$	$b \equiv 52a^5 + 158a^4 + 69a^3 + 54a^2 + 187a + 135$
		2	6	$x^2 + 40x + 99$	cubic
		3	6	$x^6+175x^5+47x^4+39x^3+188x^2+151x+31$	$b \equiv 125a^5 + 174a^4 + 149a^3 + 76a^2 + 90a + 94$
		4	6	$x^6+175x^5+47x^4+39x^3+188x^2+151x+31$	$b \equiv 34a^5 + 90a^4 + 204a^3 + 81a^2 + 145a + 150$
251	219	1	2	$x^2 + 121x + 50$	$b \equiv 196a + 171$
		2	2	$x^2 + 121x + 50$	$b \equiv 231$
		3	2	$x^2 + 144x + 228$	$b \equiv 76a + 60$
		4	2	$x^2 + 121x + 50$	$b \equiv 55a + 49$
		5	2	$x^2 + 144x + 228$	$b \equiv 175a + 160$
		6	2	$x^2 + 144x + 228$	$b \equiv 231$
		7	4	$x^4 + 241x^3 + 231x^2 + 27x + 3$	$b \equiv 28a^3 + 6a^2 + 242a + 208$
		8	4	$x^4 + 241x^3 + 231x^2 + 27x + 3$	$b \equiv 231$
		9	4	$x^4 + 241x^3 + 231x^2 + 27x + 3$	$b \equiv 223a^3 + 245a^2 + 9a + 12$
271	10	1	8	$x^8 + 4x^7 + 243x^6 + 103x^5 + 131x^4 + 18x^3 + 27x^2 + 62x + 144$	$b \equiv 46a^7+135a^6+61a^5+203a^4+261a^3 + 251a^2 + 166a + 196$
		2	8	$x^8 + 4x^7 + 243x^6 + 103x^5 + 131x^4 + 18x^3 + 27x^2 + 62x + 144$	$b \equiv 57$
		3	8	$x^8 + 4x^7 + 243x^6 + 103x^5 + 131x^4 + 18x^3 + 27x^2 + 62x + 144$	$b \equiv 225a^7 + 136a^6 + 210a^5 + 68a^4 + 10a^3 + 20a^2 + 105a + 234$
311	36	1	1	$x + 301$	$b \equiv 160$
		2	1	$x + 122$	$b \equiv 160$
		3	1	$x + 249$	$b \equiv 160$
		4	1	$x + 44$	$b \equiv 160$
		5	2	$x + 249$	quadratic
		6	2	$x + 122$	quadratic
		7	2	$x + 44$	quadratic

q	ζ_q	k	$f(\mathfrak{Q}_k)$	h_k	residue of b
		8	2	$x+301$	quadratic
		9	4	$x^4+221x^3+90x^2+50x+25$	$b\equiv 206a^3+232a^2+166a+73$
		10	4	$x^4+221x^3+90x^2+50x+25$	$b\equiv 105a^3+79a^2+145a+15$
		11	4	$x^4+221x^3+90x^2+50x+25$	$b\equiv 160$
331	64	1	4	$x^4+253x^3+279x^2+96x+39$	$b\equiv 258$
		2	4	$x^4+253x^3+279x^2+96x+39$	$b\equiv 25$
		3	4	$x^4+82x^3+131x^2+316x+239$	$b\equiv 312$
		4	4	$x^4+82x^3+131x^2+316x+239$	$b\equiv 25$
		5	4	$x^4+82x^3+131x^2+316x+239$	$b\equiv 258$
		6	4	$x^4+253x^3+279x^2+96x+39$	$b\equiv 312$
401	72	1	3	$x+276$	cubic
		2	21	$x^7+129x^6+57x^5+140x^4+117x^3+348x^2+230x+200$	cubic
431	95	1	3	$x+154$	cubic
		2	21	$x^7+281x^6+229x^5+339x^4+236x^3+420x^2+379x+201$	cubic
461	88	1	1	$x+122$	$b\equiv 367$
		2	2	$x+122$	quadratic
		3	3	$x^3+354x^2+309x+22$	$b\equiv 367$
		4	4	$x^4+450x^3+435x^2+253x+405$	$b\equiv 97a^3+253a^2+241a+279$
		5	4	$x^4+450x^3+435x^2+253x+405$	$b\equiv 367$
		6	4	$x^4+450x^3+435x^2+253x+405$	$b\equiv 364a^3+208a^2+220a+183$
		7	6	$x^3+354x^2+309x+22$	quadratic
541	48	1	3	$x+52$	cubic
		2	21	$x^7+493x^6+304x^5+254x^4+177x^3+12x^2+216x+190$	cubic
601	423	1	1	$x+350$	$b\equiv 127$
		2	1	$x+545$	$b\equiv 127$
		3	2	$x+545$	quadratic
		4	2	$x+350$	quadratic
		5	6	$x^6+311x^5+258x^4+565x^3+213x^2+416x+192$	$b\equiv 127$
		6	6	$x^6+311x^5+258x^4+565x^3+213x^2+416x+192$	$b\equiv 85a^5+502a^4+469a^3+269a^2+185a+169$
		7	6	$x^6+311x^5+258x^4+565x^3+213x^2+416x+192$	$b\equiv 516a^5+99a^4+132a^3+332a^2+416a+184$
631	242	1	3	$x^3+152x^2+58x+174$	$b\equiv 124a^2+330a+387$
		2	3	$x^3+152x^2+58x+174$	$b\equiv 47a^2+442a+423$
		3	3	$x^3+152x^2+58x+174$	$b\equiv 460a^2+490a+325$
		4	3	$x+494$	cubic
		5	6	$x^2+325x+318$	cubic
		6	6	$x^2+295x+430$	cubic
661	247	1	2	$x^2+300x+466$	$b\equiv 657$
		2	2	$x^2+300x+466$	$b\equiv 129a+447$
		3	2	$x^2+300x+466$	$b\equiv 532a+85$
		4	3	$x^3+493x^2+437x+378$	$b\equiv 657$
		5	3	$x^3+533x^2+265x+305$	$b\equiv 657$
		6	6	$x^3+533x^2+265x+305$	quadratic
		7	6	$x^3+493x^2+437x+378$	quadratic

A.4. **The symbol matrices.** Table 7 gives the matrices M_q. Each row is written as a string of 24 digits, the entries $\chi_{\mathfrak{Q}_k}(B_1), \ldots, \chi_{\mathfrak{Q}_k}(B_{24})$ in blocks of six.

A.5. **The sets $I(q)$.** The vectors $(x_1, \ldots, x_m)$ of each $I(q)$ are listed in lexicographic order, each written as the string $x_1 x_2 \cdots x_m$; coordinate k refers to the prime $\mathfrak{Q}_k$ of Table 6.

$q = 11$, $m = 4$, $\#I(11) = 1$: 1124

$q = 101$, $m = 7$, $\#I(101) = 16$: 0023440 0024304 0342211 0431212 0432121 1241442 1244124 2003440 2004304 2320443 2324034 3401212 3402121 4211442 4214124 4302211

$q = 131$, $m = 9$, $\#I(131) = 112$: 011110202 011110220 013442202 013442220 022401234 022401243 023342234 023342243 023441301 023441310 033242234 033242243 042201234 042201243 043142202 043142220 043241301 043241310 101101202 101101220 104324202 104324220 110110202 110110220 111001202 111001220 124322414 124322441 134024202 134024220 134222414 134222441 203324234 203324243 204210234 204210243 204314301 204314310 213422414 213422441 220401234 220401243 224010234 224010243 224411103 224411130 233024234 233024243 233321013 233321031 233420144 234014301 234014310 240201234 240201243 243122414 243122441 243320144 244211103 244211130 302324234 302324243 310442202 310442220 312422414 312422441 320342234 320342243 320441301 320441310 323312013 323312031 324302144 330242234 330242243 332024234 332024243 332321013 332321031 332420144 333212013 333212031 334202144 340142202 340142220 340241301 340241310 342122414 342122441 342320144 401324202 401324220 402210234 402210243 402314301 402314310 421322414 421322441 422010234 422010243 422411103 422411130 423302144 431024202 431024220 431222414 431222441 432014301 432014310 433202144 442211103 442211130

$q = 181$, $m = 11$, $\#I(181) = 59$: 00010411303 00013411003 01211204444 01214204144 02111240444 02114240144 03312333203 03313033430 03314033330 03411332344 03413332144 04311323344 04313323144 10201214444 10204214144 11200304421 11204304021 11300303412 11304303012 12001241444 12004241144 12100340421 12104340021 12201344312 12203344112 13100330412 13104330012 20141210444 20144210144 21041201444 21044201144 21140300421 21144300021 21241304312 21243304112 22141340312 22143340112 30332313203 30333013430 30334013330 30431312344 30433312144 31130300412 31134300012 33032331203 33033031430 33034031330 33430432303 33433432003 34031321344 34033321144 34330423303 34333423003 40321313344 40323313144 43021331344 43023331144 43320433303 43323433003

$q = 211$, $m = 4$, $\#I(211) = 24$: 0201 0210 0224 0233 0242 1200 1214 1223 1232 1241 2204 2213 2231 2240 3203 3212 3221 3230 3244 4202 4211 4220 4234 4243

$q = 251$, $m = 9$, $\#I(251) = 172$: 011431000 012430113 012430311 013411000 013420113 013420311 013443131 014433131 020332131 023302131 023334014 023334410 031222023 031222320 031240041 031240140 032212023 032212320 032230244 032230442 033220244 033220442 033243014 033243410 034210041 034210140 034233014 034233410 041131023 041131320 043111023 043111320 100423041 100423140 101422104 101422401 102403041 102403140 102412104 102412401 110314023 110314320 110341000 111304023 111304320 112321203 112321302 114301000 120223023 120223320 121240104 121240401 122203023 122203320 124210104 124210401 141031023 141031320 143011023 143011320 200323244 200323442 200341113 200341311 202303244 202303442 202321014 202321410 204301113 204301311 211231203 211231302 212230014 212230410 213211203 213211302 213220014 213220410 213243032 213243230 214233032 214233230 220123023 220123320 221140104 221140401 222103023 222103320 224110104 224110401 231022023 231022320 231040041 231040140 232012023 232012320 232030244 232030442 233020244 233020442 233043014 233043410 234010041 234010140 234033014 234033410 244442014 244442410 300223244 300223442 300241113 300241311 302203244 302203442 302221014 302221410 304201113 304201311 310114023 310114320 310141000 311104023 311104320 312121203 312121302 314101000 320032131 323002131 323034014 323034410 330423014 330423410 330441131 332403014 332403410 332421032 332421230 334401131 340332014 340332410 343302014 343302410 400123041 400123140 401122104 401122401 402103041 402103140 402112104 402112401 411031000 412030113 412030311 413011000 413020113 413020311 413043131 414033131 422444014 422444410 424424014 424424410 430323014 430323410 430341131 432303014 432303410 432321032 432321230 434301131 444242014 444242410

$q = 271$, $m = 3$, $\#I(271) = 5$: 020 124 223 322 421

$q = 311$, $m = 11$, $\#I(311) = 240$: 00131242044 00131242404 00314212044 00314212404 01032142044 01032142404 01230142012 01230142102 01230142242 01230142422 01240132341 01240132431 01304122044 01304122404 01324102012 01324102102 01324102242 01324102422 01344132030 01344132300 01423102341 01423102431 01433142030 01433142300 02131042012 02131042102 02131042242 02131042422 02141032341

TABLE 7. The symbol matrices $M_q = \left(\chi_{\mathfrak{Q}_k}(B_j)\right)_{k,j}$; row k corresponds to $\mathfrak{Q}_k$ of Table 6.

q	k	row k of M_q	q	k	row k of M_q
11	1	144001 142242 010001 404011	311	1	311321 410132 100114 413410
	2	043014 144314 000033 022200		2	321040 222331 103222 340404
	3	144040 242132 010414 443102		3	142243 341213 134203 002413
	4	423444 024144 030112 241242		4	244130 300423 123321 310100
101	1	200013 143414 104402 411324		5	011441 111124 401110 244402
	2	303444 213421 344214 433220		6	003421 103024 402331 210421
	3	321021 223414 142330 424010		7	013000 400112 422431 341242
	4	210331 203010 220031 324004		8	002020 404332 420001 434231
	5	230214 040022 204012 400441		9	303243 344331 323100 340023
	6	132313 024112 341234 212001		10	032020 210240 300334 243401
	7	303223 213111 310442 411110		11	004042 430013 442003 443123
131	1	224021 323221 200342 200224	331	1	240331 440413 012204 431044
	2	411130 422214 222323 032044		2	233024 043042 132300 432444
	3	340132 004334 242302 302410		3	011042 411211 421423 340101
	4	020013 212041 242210 434410		4	033232 233422 131402 220221
	5	333001 124221 113201 014133		5	003013 401242 043301 124011
	6	412310 414203 131004 212340		6	201134 243441 421430 113344
	7	031041 314421 232204 033302	401	1	312311 313043 010134 421200
	8	003233 123001 441342 004440		2	321022 024234 040421 134300
	9	002440 300120 442242 444412	431	1	131203 134344 010403 404202
181	1	112122 200331 413131 212421		2	441024 142322 040102 101303
	2	333333 032010 400024 420014	461	1	140404 023221 010120 001432
	3	023103 101232 421220 033413		2	211202 434241 010304 330401
	4	032333 043342 102013 203144		3	431341 004232 033213 230123
	5	242224 343331 142321 423001		4	440032 412004 040310 142440
	6	144034 212423 312113 021400		5	240421 144241 012222 324000
	7	422211 122234 100244 124104		6	332302 010021 023100 414001
	8	143334 414223 104144 314121		7	044241 422144 032341 224213
	9	442041 422333 131214 324311	541	1	420114 021441 040033 123334
	10	201413 420423 222324 021422		2	241002 142442 010022 432221
	11	342243 021443 323032 130324	601	1	230421 311141 300112 422221
211	1	014311 000112 040344 430414		2	434140 431122 321234 321211
	2	242424 341241 010402 404112		3	240343 443022 214204 403213
	3	123443 444343 034104 302143		4	411203 131001 240102 223111
	4	303104 044303 021210 424441		5	303430 242321 300113 011343
251	1	230434 011221 234434 241222		6	400324 304442 144303 224343
	2	320131 143324 101334 343020		7	342304 304222 141002 011223
	3	432321 231334 201213 041222	631	1	230014 304243 001043 214004
	4	340421 241400 240312 302220		2	442001 133241 032340 201441
	5	220312 244313 244334 002142		3	402433 342420 042240 421342
	6	403010 330043 120330 444434		4	111412 212042 040034 123424
	7	442332 301142 423002 314434		5	002213 104414 000232 022143
	8	331044 203422 200340 022321		6	234103 134244 040321 134311
	9	042210 014304 402421 011200	661	1	001423 123341 234420 444042
271	1	430221 432124 014124 312024		2	311110 434124 400002 424313
	2	342244 240011 000000 000000		3	322321 233310 421220 203114
	3	233140 430142 041431 243031		4	334034 100114 342314 213120
				5	434424 134030 321124 301333
				6	134031 133022 214442 440330
				7	212100 343224 233143 140413

02141032431 02314012012 02314012102 02314012242 02314012422 02413012341 02413012431 03012412044 03012412404 03101422044 03101422404 03121402012 03121402102 03121402242 03121402422 03141432030 03141432300 03210412012 03210412102 03210412242 03210412422 03413412030 03413412300 04121302341 04121302431 04131342030 04131342300 04210312341 04210312431 04314312030 04314312300 10032241044 10032241404 10230241012 10230241102 10230241242 10230241422 10240231341 10240231431 10304221044 10304221404 10324201012 10324201102 10324201242 10324201422 10344231030 10344231300 10423201341 10423201431 10433241030 10433241300 12032041012 12032041102 12032041242 12032041422 12042031341 12042031431 12304021012 12304021102 12304021242 12304021422 12403021341 12403021431 12443031012 12443031102 13002421044 13002421404 13022401012 13022401102 13022401242 13022401422 13042431030 13042431300 13200421012 13200421102 13200421242 13200421422 13403421030 13403421300 14022301341 14022301431 14032341030 14032341300 14200321341 14200321431 14240331012 14240331102 14304321030 14304321300 14423301012 14423301102 20131240012 20131240102 20131240242 20131240422 20141230341 20141230431 20314210012 20314210102 20314210242 20314210422 20413210341 20413210431 21032140012 21032140102 21032140242 21032140422 21042130341 21042130431 21304120012 21304120102 21304120242 21304120422 21403120341 21403120431 21443130012 21443130102 23012410012 23012410102 23012410242 23012410422 23101420012 23101420102 23101420242 23101420422 24012310341 24012310431 24101320341 24101320431 24141330012 24141330102 24413310012 24413310102 30012214044 30012214404 30101224044 30101224404 30121204012 30121204102 30121204242 30121204422 30141234030 30141234300 30210214012 30210214102 30210214242 30210214422 30413214030 30413214300 31002124044 31002124404 31022104012 31022104102 31022104242 31022104422 31042134030 31042134300 31200124012 31200124102 31200124242 31200124422 31403124030 31403124300 32012014012 32012014102 32012014242 32012014422 32101024012 32101024102 32101024242 32101024422 34012314030 34012314300 34101324030 34101324300 40121203341 40121203431 40131243030 40131243300 40210213341 40210213431 40314213030 40314213300 41022103341 41022103431 41032143030 41032143300 41200123341 41200123431 41240133012 41240133102 41304123030 41304123300 41423103012 41423103102 42012013341 42012013431 42101023341 42101023431 42141033012 42141033102 42413013012 42413013102 43012413030 43012413300 43101423030 43101423300 44121303012 44121303102 44210313012 44210313102

$q = 331$, $m = 6$, $\#I(331) = 21$: 001124 012023 023422 034321 040220 102113 113012 130310 203102 214001 220400 231304 242203 310040 321444 332343 343242 400130 422433 433332 444231

$q = 401$, $m = 2$, $\#I(401) = 1$: 12

$q = 431$, $m = 2$, $\#I(431) = 1$: 00

$q = 461$, $m = 7$, $\#I(461) = 84$: 0103243 0104233 0110132 0111122 0112112 0113102 0114142 0120041 0121031 0123011 0124001 0131440 0132430 0133420 0134410 0143334 1001123 1002113 1010042 1014002 1021441 1022431 1023421 1024411 1033330 1040224 1041214 1042204 1043244 1044234 2400043 2401033 2402023 2403013 2404003 2411442 2412432 2413422 2414412 2422341 2423331 2424321 2433240 2434230 2440134 2441124 2442114 2443104 3300403 3310312 3311302 3312342 3313332 3314322 3320221 3321211 3322201 3323241 3324231 3331120 3332110 3340044 3342024 3344004 4200313 4201303 4203333 4211212 4213242 4214232 4220131 4221121 4222111 4223101 4230040 4231030 4232020 4233010 4234000 4240404 4241444 4242434 4243424 4244414

$q = 541$, $m = 2$, $\#I(541) = 1$: 12

$q = 601$, $m = 7$, $\#I(601) = 120$: 0022200 0022214 0022223 0022232 0022241 0112101 0112110 0112124 0112133 0112142 0202002 0202020 0202034 0202043 0342403 0342412 0342421 0342430 0342444 0432304 0432313 0432322 0432331 0432340 1021101 1021110 1021124 1021133 1021142 1111002 1111011 1111020 1201403 1201412 1201421 1201430 1201444 1341304 1341313 1341322 1341331 1341340 1431200 1431214 1431223 1431232 1431241 2020002 2020020 2020034 2020043 2110403 2110412 2110421 2110430 2110444 2200304 2200313 2200322 2200331 2200340 2340200 2340214 2340223 2340232 2340241 2430101 2430110 2430124 2430133 2430142 3024403 3024412 3024421 3024430 3024444 3114304 3114313 3114322 3114331 3114340 3204200 3204214 3204223 3204232 3204241 3344101 3344110 3344124 3344142 3434002 3434011 3434020 3434034 3434043 4023304 4023313 4023322 4023331 4023340 4113200 4113214 4113223 4113232 4113241 4203101 4203110 4203124 4203133 4203142 4343002 4343011 4343020 4343034 4343043 4433403 4433412 4433421 4433430 4433444

$q = 631$, $m = 6$, $\#I(631) = 25$: 004311 013311 022311 031311 040311 103311 112311 121311 130311 144311 202311 211311 220311 234311 243311 301311 310311 324311 333311 342311 400311 414311 423311 432311 441311

$q = 661$, $m = 7$, $\#I(661) = 68$: 0020443 0021302 0022211 0023120 0024034 0110443 0114034 0200443 0201302 0202211 0203120 0204034 1010303 1011212 1012121 1013030 1100303 1101212 1102121 1103030 1240303 1241212 1242121 1243030 1331212 1332121 1420303 1421212 1422121 1423030 2000213 2002031 2141122 2230213 2232031 2320213 2322031 2411122 3040123 3041032 3042441 3044214 3130123 3131032 3220123 3221032 3310123 3311032 3400123 3401032 3402441 3404214 4031442 4032301 4033210 4034124 4121442 4122301 4123210 4124124 4211442 4212301 4213210 4214124 4301442 4302301 4303210 4304124

A.6. **The affine space and the last stages of the sieve.** The affine space $\mathcal{A}$ of Theorem 7.1, cut out by (N) and (V), is $\{c_0 + \sum_{k=1}^{10} \lambda_k d_k : \lambda \in \mathbb{F}_5^{10}\}$ with

$$c_0 = (302030\,000410\,030430\,000000),$$

$$\begin{aligned} d_1 &= (000000\,004001\,000000\,000000) & d_2 &= (000000\,000000\,100000\,000000)\\ d_3 &= (000000\,000000\,001000\,000000) & d_4 &= (000000\,000410\,020131\,000000)\\ d_5 &= (000000\,000000\,010000\,100000) & d_6 &= (000000\,000000\,000010\,010000)\\ d_7 &= (000000\,000000\,010010\,001000) & d_8 &= (000000\,000410\,030100\,000100)\\ d_9 &= (000000\,000140\,010010\,000010) & d_{10} &= (000000\,000000\,040100\,000001) \end{aligned} \tag{A.2}$$

written in blocks of six coordinates. Table 8 lists the vectors that survive the conditions at 181, 311 and 131.

	c (in blocks of six coordinates)	$M_{251}\,c$	in $I(251)$?
1	302030 000320 011031 244441	222112131	no
2	302030 000320 041432 301231	343320032	no
3	302030 000320 043300 001212	232044104	no
4	302030 000320 044042 213014	413002343	no
5	302030 000320 100103 424024	034210343	no
6	302030 000320 424131 241224	440232410	no
7	302030 004411 440432 434023	211213131	no
8	302030 003002 121342 143032	001022302	no
9	302030 003002 422133 003430	404124131	no
10	302030 002143 032234 342123	102430320	no
11	302030 002143 004230 043132	423420401	no
12	302030 002143 112440 031020	334410041	no
13	302030 002143 114411 403420	214224122	no
14	302030 002143 440111 141204	234042122	no
15	302030 002143 441223 104114	331413014	no
16	302030 001234 101442 432003	030223410	no
17	302030 001234 131344 411020	213243230	yes
18	302030 001234 230234 044301	400141113	no
19	302030 001234 204033 330231	133111230	no

TABLE 8. The 19 vectors $c \in \mathcal{A}$ with $M_q c \in I(q)$ for $q = 181, 311, 131$, and their images under M_{251}, written as digit strings. Only the 17th satisfies the condition at 251; its image under M_{101} is $1423030 \notin I(101)$.

APPENDIX B. THE CLASS NUMBER OF L_{24}

This appendix proves Theorem 6.1. Minkowski's bound for L_{24} is about $1.42 \cdot 10^{15}$, so a proof that examines every prime ideal below it is out of reach. We use instead a criterion of Belabas, Diaz y Diaz and Friedman [1, Theorem 5.1], deduced from Weil's explicit formula, under which it is enough to examine the prime ideals of norm at most 10^7. In this appendix the letters h, g, c, m, n, f, F, S_i, T, L, χ, Φ and $\mathfrak{p}$ denote the objects defined below, not those of the same or similar names in the body of the paper.

B.1. **The criterion.** Let K be a number field of degree n, with r_1 real places, r_2 complex places and discriminant d_K. For a prime ideal $\mathfrak{p}$ of K let $\mathrm{N}\,\mathfrak{p}$ be its absolute norm, and let $\gamma = 0.5772\ldots$ be Euler's constant. Let $c > 0$, let $J \geq 1$, and let $a_0, \ldots, a_{J-1}$ be real numbers, not all zero. Put

$$h(y) = \sum_{j=0}^{J-1} a_j \cos\Big(\frac{2\pi j y}{c}\Big) \ \text{ for } |y| \leq \frac{c}{2}, \qquad h(y) = 0 \ \text{ for } |y| > \frac{c}{2}, \tag{B.1}$$

and let $g = h * h$, that is, $g(x) = \int_{\mathbb{R}} h(y)h(x-y)\,dy$. Then g is real, even and continuous, $g(x) = 0$ for $|x| \geq c$, and $g(0) = \int_{\mathbb{R}} h^2 > 0$. Put $\tilde{g} = g/g(0)$, let $\kappa(x) = r_1/(1+\cosh x) + n/\sinh x$ for $x > 0$, and

$$R = r_1 + n(\gamma + \log 4\pi) - \log|d_K| - \int_0^\infty (1 - \tilde{g}(x))\kappa(x)\,dx \\ + \sum_{\mathfrak{p}} \sum_{\substack{m \geq 1 \\ \mathrm{N}\,\mathfrak{p}^m < e^c}} \frac{4\log \mathrm{N}\,\mathfrak{p}}{\mathrm{N}\,\mathfrak{p}^m + 1}\,\tilde{g}(m \log \mathrm{N}\,\mathfrak{p}), \tag{B.2}$$

where $\mathfrak{p}$ runs over the prime ideals of K. The integral converges: its integrand is bounded near 0, because g is Lipschitz, and equals $\kappa(x)$ for $x \geq c$. The number R depends only on K, c and the a_j, not on the class group of K.

Proposition B.1 (Belabas, Diaz y Diaz and Friedman)**.** *If $R > 0$, then the classes of the prime ideals of K of norm less than e^c generate the class group of K.*

Proof. This is [1, Theorem 5.1] with $T = e^c$ and f the restriction of $\tilde{g}$ to $[0,\infty)$: since $2\cosh^2(x/2) = 1 + \cosh x$, the inequality (16) of [1] is $R > 0$. The hypotheses of that theorem hold. The function f is supported on $[0,c]$ and $f(0) = 1$. Its Fourier cosine transform is $2\int_0^\infty \tilde{g}(x)\cos(xt)\,dx = \hat{h}(t)^2/g(0) \geq 0$, where $\hat{h}(t) = \int_{\mathbb{R}} h(y)e^{-ity}\,dy$ is real because h is real and even. And $F(x) = \tilde{g}(x)/\cosh(x/2)$ is even, continuous, compactly supported, and real-analytic on $[0,c]$ (by (B.4) below) and on $[c,\infty)$, so it satisfies the conditions of Weil's formula in the form of Poitou [18, Théorème, p. 6-06].

For the reader's convenience we recall the argument. Let H be the subgroup of the class group generated by the classes of the prime ideals of norm less than e^c, and suppose that H is a proper subgroup. Then there is a nontrivial character χ of the class group that is trivial on H. Put $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$ and $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$, and let $\Lambda(s,\chi) = |d_K|^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}L(s,\chi)$ be the completed L-function. Since χ is unramified at every place, $\Lambda(s,\chi)$ has the same gamma factors as the Dedekind zeta function of K. It is entire, of order 1, and satisfies $\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\bar{\chi})$ with $|W(\chi)| = 1$. Poitou's proof of Weil's formula for the Dedekind zeta function [18, §1], including his bound on the horizontal segments of the contour (his Proposition 1), carries over to $\Lambda(s,\chi)$ with two changes: the functional equation relates $\Lambda(s,\chi)$ to $\Lambda(1-s,\bar{\chi})$, and there is no pole. With $\Phi(s) = \int_{\mathbb{R}} F(x)e^{(s-1/2)x}\,dx$ it gives

$$\sum_\rho \Phi(\rho) = \log|d_K| - A(F) - 2\sum_{\mathfrak{p}} \sum_{m \geq 1} \mathrm{Re}\,(\chi(\mathfrak{p})^m)\frac{\log \mathrm{N}\,\mathfrak{p}}{\mathrm{N}\,\mathfrak{p}^{m/2}} F(m \log \mathrm{N}\,\mathfrak{p}), \tag{B.3}$$

where ρ runs over the zeros of $L(s,\chi)$ with $0 < \mathrm{Re}\,\rho < 1$, counted with multiplicity and summed symmetrically in $\mathrm{Im}\,\rho$, and

$$A(F) = \frac{\pi r_1}{2} + n(\gamma + \log 8\pi) - r_1 \int_0^\infty \frac{1 - F(x)}{2\cosh(x/2)}\,dx - n\int_0^\infty \frac{1-F(x)}{2\sinh(x/2)}\,dx$$

(see also [26], [16, Chapter XVII] and [1, (3)]). A term of the prime sum with $F(m\log \mathrm{N}\,\mathfrak{p}) \neq 0$ has $\mathrm{N}\,\mathfrak{p} \leq \mathrm{N}\,\mathfrak{p}^m < e^c$, so $\chi(\mathfrak{p}) = 1$ there. On the other side, $\operatorname{Re}\Phi(\rho) \geq 0$ whenever $0 < \operatorname{Re}\rho < 1$. Indeed, write $\rho = \frac{1}{2} + \sigma + i\tau$ with $|\sigma| < \frac{1}{2}$. Then

$$\operatorname{Re}\Phi(\rho) = \int_{\mathbb{R}} \tilde{g}(x)\mu_\sigma(x)\cos(\tau x)\,dx \qquad \text{with } \mu_\sigma(x) = \frac{\cosh(\sigma x)}{\cosh(x/2)}.$$

The Fourier transform of μ_σ is $2\pi\cos(\pi\sigma)\cosh(\pi\xi)/|\cosh(\pi(\xi+i\sigma))|^2 > 0$, and $\hat{g} = \hat{h}^2 \geq 0$, so Parseval's formula gives $\operatorname{Re}\Phi(\rho) \geq 0$. (Alternatively, positivity on the strip follows from positivity on the line $\operatorname{Re} s = 1$ by the maximum principle [18, p. 6-08], [1, §5].) Finally, $2N^{-m/2}/\cosh(\frac{m}{2}\log N) = 4/(N^m+1)$ for $N = \mathrm{N}\,\mathfrak{p}$, and the identities

$$\int_0^\infty (1-\operatorname{sech} u)\operatorname{sech} u\,du = \frac{\pi}{2} - 1, \qquad \int_0^\infty \frac{1-\operatorname{sech} u}{\sinh u}\,du = \log 2$$

give $A(F) = r_1 + n(\gamma + \log 4\pi) - \int_0^\infty (1-\tilde{g})\kappa$. So the real part of the right side of (B.3) is $-R$, and $0 \leq -R$, which contradicts $R > 0$. □

For the computation we use the following closed form, which is elementary (substitute $y = u + x/2$ and use the product-to-sum formulas). Put $\omega_j = 2\pi j/c$. For $0 \leq x \leq c$,

$$g(x) = (c-x)\sum_{j=0}^{J-1} \beta_j \cos(\omega_j x) + \sum_{i=1}^{J-1} S_i \sin(\omega_i x), \tag{B.4}$$

with $\beta_0 = a_0^2$, $\beta_j = a_j^2/2$ for $j \geq 1$, and

$$S_i = -\frac{a_i^2}{2\omega_i} - 2a_i \sum_{\substack{0\leq k<J \\ k\neq i}} (-1)^{i+k} a_k \frac{\omega_i}{\omega_i^2 - \omega_k^2}.$$

B.2. **The computation for L_{24}.** We apply Proposition B.1 to $K = L_{24}$, with $n = 24$, $r_1 = 2$, $r_2 = 11$ and $d_K = -2^{44}\cdot 5^{20}\cdot 7^{23}$ (Lemma 2.4), with $T = 10^7$ and $c = \log T$, and with $J = 20$ and the coefficients a_j of Table 9. The a_j were found as follows. Both $g(0)$ and $R\,g(0)$ are quadratic forms in $(a_0, \dots, a_{J-1})$, so the coefficients that maximize R form the top eigenvector of a generalized symmetric eigenvalue problem. We solved it in floating point for $J = 20$ and $c = \log 10^7$, normalized the eigenvector to $a_0 = 1$ and rounded it to eight decimal places. The proof uses only the printed values, read as exact rational numbers. The same floating-point computation shows that for $J = 20$ the maximum of R changes sign between $c = 15.75$ and $c = 16$, which is why we took the round bound $T = 10^7$, with $c = 16.118\ldots$.

j	a_j	j	a_j	j	a_j	j	a_j
0	1	5	0.02000542	10	−0.01007476	15	0.00413216
1	0.15211830	6	−0.01334957	11	0.00896303	16	−0.00403606
2	−0.08506698	7	0.00970009	12	−0.00736544	17	0.00363395
3	0.04674648	8	−0.00852986	13	0.00616254	18	−0.00327830
4	−0.02962281	9	0.00863041	14	−0.00513556	19	0.00335562

TABLE 9. The coefficients a_j of the function h used for L_{24} ($J = 20$, $c = \log 10^7$).

(a) The prime ideals. Since 10^7 is not a prime power, the condition $\mathrm{N}\,\mathfrak{p}^m < e^c = 10^7$ in (B.2) selects the same terms as $\mathrm{N}\,\mathfrak{p}^m \leq 10^7$, and the prime ideals in Proposition B.1 are

those of norm at most 10^7. We listed them in two ways. First, with PARI's `idealprimedec` on the maximal order of L_{24}, which is certified with `nfcertify`. Second, from the decompositions in L_8 and in $\mathbb{Q}(b)$. The polynomial $x^3 + 2x - 2$ defines $\mathbb{Q}(b)$: if y is a root of it, then $b = (-2y^2 + y - 4)/5$ is a root of ψ. The discriminant -140 of $x^3 + 2x - 2$ equals that of $\mathbb{Q}(b)$, and the index of $\mathbb{Z}[a]$ in the ring of integers of L_8 is $2^7 \cdot 5 \cdot 41$ (Lemma 2.4). So for $p \notin \{2, 5, 7, 41\}$ the prime p is unramified in $L_{24} = L_8 \otimes_{\mathbb{Q}} \mathbb{Q}(b)$, and, by the Dedekind–Kummer theorem, its residue degrees in L_8 and in $\mathbb{Q}(b)$ are the degrees of the irreducible factors modulo p of the octic polynomial in (1.6) and of $x^3 + 2x - 2$. Each pair of primes of L_8 and of $\mathbb{Q}(b)$ above p, of residue degrees d and d', gives $\gcd(d, d')$ primes of L_{24} of residue degree $\operatorname{lcm}(d, d')$. For $p \in \{2, 5, 7, 41\}$ we used `idealprimedec`. Both lists consist of the same 665 770 prime ideals, above 280 528 rational primes, and the sum in (B.2) has 666 361 terms.

(b) The value of R. We evaluated (B.2) in ball arithmetic (Arb [15], through python-flint), in which every real number is represented by an interval that is guaranteed to contain it. The function g is evaluated by (B.4). The integral is split at $\delta = 2^{-20}$ and at c. On $[\delta, c]$ it is computed by Arb's certified integration of the analytic integrand. On $[0, \delta]$ we use $\kappa(x) \le r_1/2 + n/x$ and $0 \le g(0) - g(x) \le Lx$, where the lower bound is the Cauchy–Schwarz inequality and $L = \sum_j |\beta_j|(1 + c\,\omega_j) + \sum_i |S_i|\,\omega_i$ bounds $|g'|$ on $[0, c]$ by (B.4). So this part of the integral lies between 0 and $\delta(nL + r_1 L\delta/4)/g(0)$. On $[c, \infty)$, where $g = 0$, the integral equals $r_1(1 - \tanh\frac{c}{2}) - n \log\tanh\frac{c}{2}$. At 128-bit precision this gives $R \in [0.629536,\, 0.629544]$, the computed interval rounded outward. At 200-bit precision and with $\delta = 2^{-30}$ it gives $R = 0.62954314 \pm 3.72 \cdot 10^{-9}$. The three parts of (B.2) are $r_1 + n(\gamma + \log 4\pi) - \log|d_K| = -30.84540973\ldots$, $\int_0^\infty (1 - \tilde{g})\kappa = 2.37838643\ldots$ and the prime sum $33.85333930\ldots$, with $g(0) = 16.39716346\ldots$. In particular $R > 0$.

(c) Principality. For each of the 665 770 prime ideals $\mathfrak{p}$ of (a) we found an element $\alpha \in L_{24}$ with $\alpha\mathcal{O}_{L_{24}} = \mathfrak{p}$. A candidate α was proposed by PARI's `bnfisprincipal`, from a class group computation that is proved correct only under the generalized Riemann hypothesis. This computation serves only to find α. Each candidate was then checked by exact arithmetic:

(1) the coordinates of α on an integral basis of the certified maximal order of L_{24} are integers, so α is an algebraic integer;
(2) $|\mathrm{N}_{L_{24}/\mathbb{Q}}(\alpha)| = \mathrm{N}\,\mathfrak{p}$;
(3) $v_{\mathfrak{p}}(\alpha) \ge 1$.

By (1) and (3), $\alpha\mathcal{O}_{L_{24}} = \mathfrak{p}\mathfrak{a}$ with $\mathfrak{a}$ an integral ideal, and by (2), $\mathrm{N}\,\mathfrak{a} = 1$, so $\alpha\mathcal{O}_{L_{24}} = \mathfrak{p}$. All 665 770 prime ideals pass these checks. The generators are not stored: the program deposited in [14] finds them again and repeats these exact checks in 3765 seconds on one core.

Proof of Theorem 6.1. By (b), $R > 0$, so by Proposition B.1 and (a) the classes of the prime ideals of L_{24} of norm at most 10^7 generate the class group of L_{24}. By (c) all these classes are trivial. Hence the class group of L_{24} is trivial. □

These computations were repeated by separately written programs (Appendix C.2).

Remark B.2. As a smaller example of the criterion, with the simplest test function, the same method shows without the generalized Riemann hypothesis that L_8 has class number 1. Take $K = L_8$ ($n = 8$, $r_1 = 2$, $d_K = -2^{14} \cdot 5^6 \cdot 7^7$), $J = 1$ and $a_0 = 1$, so that h is the indicator function of $[-c/2, c/2]$ and $g(x) = \max(c - |x|, 0)$, and take $T = e^c = 300$. The sum in (B.2) then runs over the 61 prime ideals of L_8 of norm less than 300 (87 terms), and

$R = 1.45103\ldots > 0$. Every prime ideal of L_8 of norm at most 1000, more than the bound 300 requires, is principal, as checked in the manner of (c).

Appendix C. Computations

C.1. **List of computational statements.** Table 10 lists the statements that rest on, or were checked by, machine computation. All arithmetic is exact: integers, rationals, polynomials, number fields given by defining polynomials, and finite fields. The one exception is the enclosure of the number R in Appendix B, which uses ball arithmetic: floating-point intervals that are guaranteed to contain the exact values. The only class group that the proof uses is that of L_{24}, determined in Appendix B by an argument that uses no unproved hypothesis.

Statement	What is computed
Lemma 2.1, (1.3), (2.2)	polynomial identities, discriminants and resultants
Lemmas 2.4 and 2.5	maximal orders of L_8 and L_{24} (`nfinit`, certified by `nfcertify`), signatures, discriminants, prime decompositions (`idealprimedec`), labels
Lemma 2.6	checked by `factorpadic` (the proof is by hand)
Proposition 5.4	the types of L_8 at the primes $q \equiv 1 \pmod 5$ up to 700 and the types of the forms of Proposition 5.2; the admissible residues, families and the sets $I(q)$
Proposition 6.2(i), Lemma 6.3	characteristic polynomials and ideal factorizations of the B_j; the valuation matrix; the symbol matrices and their ranks; the exact norm identities
Theorem 7.1	the linear algebra over $\mathbb{F}_5$ and the exhaustive enumeration of the 5^{10} vectors of $\mathcal{A}$
Remarks 7.2 and 7.3, Section 8	further runs of the sieve, and the ranks of the maps $c \mapsto M_q c$ on $\mathcal{A}$; the tests on the fibres above $\eta = -1$ and $\eta = 243$
Theorem 6.1 (Appendix B)	the prime ideals of L_{24} of norm at most 10^7 (two methods); an enclosure of R in ball arithmetic; for each of these prime ideals, a generator, checked by exact arithmetic; the corresponding computations for L_8 (Remark B.2)

Table 10. The computational statements of the paper.

The computations for Lemmas 2.4 and 2.5, Propositions 5.4 and 6.2, Lemma 6.3, and Theorem 7.1 take a few minutes in total on one core of a laptop, most of it in the exhaustive sieve. The tests of Section 8 take a few minutes each. The computations of Appendix B take about an hour and a quarter: a few minutes for each list of prime ideals and for the enclosure of R, and about an hour for the generators of the 665 770 prime ideals.

We describe how the data of Appendix A are obtained and checked. The field L_{24} is built as $L_8[x]/(x^3 + 20x^2 + 350x + 8750)$, where the cubic is the minimal polynomial of $25b$, and represented by an absolute defining polynomial of degree 24. The elements a and b are expressed in this absolute representation, and the printed elements B_j and u_i, given as polynomials in a and b, are evaluated there. The candidates B_j were found with PARI's `bnfinit` and `bnfunits`. This uses the generalized Riemann hypothesis, but only to find the elements, whose properties are then checked unconditionally: the S-unit property by characteristic polynomials and by ideal factorization, the valuations by `nfeltval`, and the independence by the rank of the symbol matrix. For the auxiliary primes, the residue fields $k(\mathfrak{q})$ and $k(\mathfrak{Q})$ are handled with `nfmodpr`. The roots of $f_{\bar\eta}$ in $k(\mathfrak{q})$ are found with `polrootsmod` and transported to $k(\mathfrak{Q})$ by lifting to L_8, embedding in L_{24} and reducing. A separate program recomputes every row of every matrix M_q from the description of the primes in Table 6 alone, by arithmetic in finite fields (`ffgen`, `ffextend`), and finds the same 97 rows.

C.2. **Independent second computations.** The following computations were repeated by separately written programs, which share with the first ones only the definitions in the text and, where stated, the printed data and the defining polynomial of L_{24}.

- *The auxiliary primes and the sets* $I(q)$ (Proposition 5.4), in Python with FLINT and explicitly constructed finite fields: the same set $\mathcal{Q}$, the same entries of Table 3 and the same sets $I(q)$. This program also checked that every vector of every $I(q)$ satisfies the relation between the symbols above a prime $\mathfrak{q}$ of L_8 and the symbol of 2 at $\mathfrak{q}$ that Proposition 3.2 implies.
- *The sieve* (Theorem 7.1) *and the tests of Section 8*, with an independent model of L_{24}, its own basis of S-units, the norm condition imposed through valuations and residue symbols in L_8, and its own labels and sets $I(q)$: the same dimensions 14 and 10, the same counts 36 875, 567, 19, 1, 0, and the same single survivor in both test fields. It also agrees with the printed valuation matrix, norm identities, matrices M_q and sets $I(q)$.
- *The class number of* L_{24} (Appendix B). Two programs, both starting from the same defining polynomial of L_{24} as the first ones, list the prime ideals of norm at most 10^7, by the Dedekind–Kummer theorem for the primes not dividing its index and, for the few others, by `idealprimedec` or a second defining polynomial, and find the same 665 770 prime ideals. Each encloses R with its own closed form for g and its own treatment of the integral, and both obtain $R = 0.62954313841571501\ldots$, with radii less than $2.5 \cdot 10^{-21}$ and $3.3 \cdot 10^{-19}$. A further program proves again that all 665 770 prime ideals are principal, with another defining polynomial of L_{24} and its own certified maximal order.

C.3. **Software.** The computations used PARI/GP 2.17.3 [17], Python 3.12 with NumPy, SciPy, SymPy and mpmath, and FLINT 3.3 [10] through python-flint 0.8, including the ball arithmetic of Arb [15] for Appendix B.

C.4. **Data availability.** The inputs, programs and outputs of all computations, with scripts that run them in order and a document that describes them, are deposited at [14]. The Lean formalization of Theorems 1.1 and 1.2 described in Section 1.6 is deposited at [13].

Declarations

Research methodology. The author designed and operated the multi-agent research system used in this work, built on Anthropic Claude Opus 5.5. The system carried out literature analysis, mathematical development and computation, with checks assigned to agents separate from those developing the arguments.

Funding. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of competing interests. The author declares no competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process. Anthropic Claude Opus 5.5 was used to draft and revise the manuscript. The author reviewed the material and takes full responsibility for the article.

References

1. Karim Belabas, Francisco Diaz y Diaz, and Eduardo Friedman, *Small generators of the ideal class group*, Math. Comp. **77** (2008), no. 262, 1185–1197, https://doi.org/10.1090/S0025-5718-07-02003-0.
2. Michael A. Bennett, Preda Mihăilescu, and Samir Siksek, *The generalized Fermat equation*, Open problems in mathematics (John Forbes Nash, Jr. and Michael Th. Rassias, eds.), Springer, Cham, 2016, https://doi.org/10.1007/978-3-319-32162-2_3, pp. 173–205.

3. Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, https://doi.org/10.1090/S0025-5718-09-02255-8.
4. Peter Chocian, *The primitive generalized Fermat equation $x^3 + y^5 = z^7$: a computer-assisted proof*, 2026, Preprint, arXiv:2609.26996v1.
5. Sander R. Dahmen, *Generalized Fermat equations with three distinct prime exponents*, 2025, Talk in the Number theory lunch seminar, Max Planck Institute for Mathematics, Bonn, 2 April 2025; abstract at https://www.mpim-bonn.mpg.de/node/13952.
6. Sander R. Dahmen and Samir Siksek, *On the generalized Fermat equation $x^5 + y^3 = z^7$*, July 2024, Working paper, https://few.vu.nl/~sdn249/GFE357.pdf.
7. Henri Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no. 3, 413–449, https://doi.org/10.1215/S0012-7094-00-10233-5.
8. Henri Darmon and Andrew Granville, *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*, Bull. Lond. Math. Soc. **27** (1995), no. 6, 513–543, https://doi.org/10.1112/blms/27.6.513.
9. Andreas-Stephan Elsenhans and John Voight, *Computing class groups and unit groups in Magma*, 2025, Preprint, arXiv:2510.05501v1.
10. The FLINT team, *FLINT: Fast Library for Number Theory, version 3.3*, 2025, https://flintlib.org.
11. Nuno Freitas, Bartosz Naskręcki, and Michael Stoll, *The generalized Fermat equation with exponents 2, 3, n*, Compos. Math. **156** (2020), no. 1, 77–113, https://doi.org/10.1112/S0010437X19007693.
12. Manvir Jaswal, *The generalized Fermat equation $X^5 + Y^3 = Z^7$*, 2026, Preprint, Zenodo, https://doi.org/10.5281/zenodo.22949749.
13. ———, *Lean formalization: the generalized Fermat equation $x^2 + y^5 = z^7$*, 2026, Zenodo, https://doi.org/10.5281/zenodo.23065698.
14. ———, *Programs and data for "The generalized Fermat equation $x^2 + y^5 = z^7$"*, 2026, Zenodo, https://doi.org/10.5281/zenodo.22983849.
15. Fredrik Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. Comput. **66** (2017), no. 8, 1281–1292, https://doi.org/10.1109/TC.2017.2690633.
16. Serge Lang, *Algebraic number theory*, second ed., Grad. Texts in Math., vol. 110, Springer-Verlag, New York, 1994.
17. The PARI Group, *PARI/GP version 2.17.3*, Univ. Bordeaux, 2025, https://pari.math.u-bordeaux.fr/.
18. Georges Poitou, *Sur les petits discriminants*, Séminaire Delange–Pisot–Poitou. Théorie des nombres **18** (1976/77), no. 1, Exp. No. 6, 1–17, http://www.numdam.org/item/SDPP_1976-1977__18_1_A6_0/.
19. Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188, https://doi.org/10.1515/crll.1997.488.141.
20. Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$*, Duke Math. J. **137** (2007), no. 1, 103–158, https://doi.org/10.1215/S0012-7094-07-13714-1.
21. Piet Hein Casper Putz, *Families of étale algebras in Magma*, 2023, GitHub repository, commit 9481cf0 (22 January 2025), https://github.com/CPutz/etale-algebra-family/tree/9481cf0.
22. ———, *A parallel program for targeted Hunter searches*, 2023, GitHub repository, commit 1c2e95d (22 January 2025), https://github.com/CPutz/hunter_search/tree/1c2e95d.
23. ———, *Enumeration of local and global étale algebras applied to generalized Fermat equations*, Ph.D. thesis, Vrije Universiteit Amsterdam, 2024, https://doi.org/10.5463/thesis.832.
24. Ashleigh Ratcliffe and Bogdan Grechuk, *Generalized Fermat equation: a survey of solved cases*, Expo. Math. **43** (2025), no. 4, Paper No. 125688, https://doi.org/10.1016/j.exmath.2025.125688; arXiv:2412.11933v2.
25. Samir Siksek and Michael Stoll, *Partial descent on hyperelliptic curves and the generalized Fermat equation $x^3 + y^4 + z^5 = 0$*, Bull. Lond. Math. Soc. **44** (2012), no. 1, 151–166, https://doi.org/10.1112/blms/bdr086.
26. André Weil, *Sur les "formules explicites" de la théorie des nombres premiers*, Comm. Sém. Math. Univ. Lund [Medd. Lunds Univ. Mat. Sem.] **Tome supplémentaire** (1952), 252–265.

Toronto, Canada
Email address: manvirjaswal@icloud.com