Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

THE 167889 EVEN LATTICES OF RANK 18 AND DISCRIMINANT 163

NOAM D. ELKIES

Abstract. We use the gluing method of Witt–Kneser and Nishiyama to find all positive-definite even lattices of rank 18 and discriminant 163. There are 167889. We then use the Minkowski–Siegel mass formula to verify that we have obtained a complete list. This also gives the enumeration of elliptic fibrations of the K3 surface X_{163} of Néron–Severi rank 20 (the largest in characteristic zero) and discriminant -163, which is the last K3 surface X for which $\mathrm{NS}(X)$ has rank 20 and all of $\mathrm{NS}(X)$ can be defined over $\mathbf{Q}$. We tabulate statistics and features of this genus of lattices, and thus of the elliptic fibrations of X_{163}. For instance, their Mordell–Weil ranks range from 1 to 11, attaining each value in this range; and the nontrivial torsion groups are $\mathbf{Z}/N\mathbf{Z}$ for $N = 2, 3, 4$, occurring $3374, 159, 23$ times respectively. We make the lattices and their invariants available for download and further study.

Keywords: even lattice, gluing method, root lattice, K3 surface

MSC(2000): Primary 11E41; Secondary 14J28, 14J27

1. Introduction

The classification of quadratic forms — equivalently, of lattices — is a longstanding problem in number theory, theoretical as well as computational, and in other branches of mathematics. (For example, this problem motivates much of the beautiful and varied mathematics in [Conway–Sloane 1999].) In this paper we report on the solution of this problem for positive-definite even lattices L of rank 18 and discriminant 163. The choice of these parameters is informed by the connection with the algebraic and arithmetic geometry of K3 surfaces: some genera of positive-definite even lattices of rank 18 biject with elliptic fibrations of K3 surfaces X of Néron–Severi rank 20, the largest possible in characteristic zero; our L's classify elliptic fibrations of the last and most complicated such X for which all the fibrations and their sections can be defined over $\mathbf{Q}$. The techniques will apply to many other such classification problems.

Little of the theory and algorithms here is new. To list the lattices, we used a gluing method attributed to Witt and Kneser in [Conway–Sloane 1999, pages 352–353], and applied in our K3 context at least since [Nishiyama 1996]; this much was already completed in January 2018, and briefly reported in [Elkies 2018]. Most of the work of verifying that our list is complete and free of duplicates uses implementations in GP [PARI 2025] of the lattice algorithms of [Plesken–Souvignier 1997]. What *is* somewhat new here is the scale: for discriminant 163 we find 167889 distinct lattices, roughly equal to the total number of lattices in the Nebe–Sloane catalogue

Date: June 5, 2026.

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

[Nebe–Sloane 2026], with a total Minkowski mass $\sum_L 1/\#\mathrm{Aut}\, L$ of about 2.2. An even larger genus (374062 lattices of rank 28 and discriminant 1), with a much larger mass (104+), was recently reported in [Allombert–Chenevier 2025]; but this computation was much longer ("the total CPU time was about 72 years") and more complicated, even using some optimizations specific to lattices of discriminant 1. Even more recently [Chenevier–Taïbi 2026], much more extensive optimization reduced this to "about a week", and made feasible the computation of the even huger genus of 38966352 lattices of rank 29 and discriminant 1 in "about 20 months of CPU time"; even checking that this list is complete is an 80-day computation. But the calculations reported here took only a few CPU-hours once all the pieces were in place, so there is still considerable scope for extending them to much larger genera of positive-definite forms of rank up to about 20. The challenge would be not so much carrying out the computation as ordering and managing the resulting flood of data.

The rest of the paper is organized as follows. We start (§2) with a review of the definitions and results that we shall need for the gluing method, concluding with a brief outline of the correspondence between our lattices L and elliptic fibrations of the K3 surface X_{163}. We proceed (§3) to carry out the gluing analysis that reduces our classification problem to listing the $\mathrm{Aut}(M)$-orbits of vectors $v^* \in M^*$ of norm $\langle v^*, v^*\rangle = 163/4$ for each of the 16 positive-definite even lattices M of rank 19 and discriminant 4 (Table 2), and state our main result (Theorem 6). The next two sections are devoted to the computation of the lists of vectors v^* and lattices L (§4) and the verification that the resulting L list is complete and free of duplicates (§5). Along the way we report on the counts of positive-definite even lattices of rank 18 and discriminant p for each prime $p = 8k + 3 \le 163$ (Table 3). Finally we tabulate various statistics and features of our results (§6), and describe the files of data, such as Gram matrices and lattice invariants, that we have shared online (§7).

2. Lattices and gluing

2.1. **Lattice preliminaries.**

2.1.1. *Definition of a lattice; Gram matrix; signature* (r_+, r_-). By a *lattice* $L = (L, \langle\cdot,\cdot\rangle)$ we mean a free abelian group L of finite rank $\mathrm{rk}(L)$ together with a symmetric bilinear pairing $\langle\cdot,\cdot\rangle : L \times L \to \mathbf{R}$. Given a $\mathbf{Z}$-basis $B = (e_1, \ldots, e_r)$ for L, the pairing is determined by the *Gram matrix* $G = G_B = (\langle e_i, e_j\rangle)_{i,j=1}^r$; the *discriminant* $\mathrm{disc}\, L$ is $\det(G_B)$ for any choice of $\mathbf{Z}$-basis B. We generally assume that L is *nondegenerate*, meaning that $\mathrm{disc}\, L \neq 0$, or equivalently that the extension of $\langle\cdot,\cdot\rangle$ to a symmetric bilinear form on $L_{\mathbf{R}} := L \otimes_{\mathbf{Z}} \mathbf{R}$ is nondegenerate. We call the quadratic form $v \mapsto \langle v, v\rangle$ on $L_{\mathbf{R}}$ the *norm* associated to the pairing $\langle\cdot,\cdot\rangle$. We denote by $(r_+, r_-) = (r_+(L), r_-(L))$ the signature of this form, so r_+ and r_- are the dimensions of the maximal positive- and negative-definite subspaces of $L_{\mathbf{R}}$, and $r_+ + r_- = \dim L_{\mathbf{R}} = \mathrm{rk}(L)$.

2.1.2. *Rational, integral, and even lattices; characteristic vectors and the mod* 8 *invariant.* We say L is *rational* if $\langle v, v'\rangle \in \mathbf{Q}$ for all $v, v' \in L$, and *integral* if $\langle v, v'\rangle \in \mathbf{Z}$ for all $v, v' \in L$; equivalently, if all the entries of G are rational (resp. integral). If L is integral then the parity-of-norm map $L \to \mathbf{Z}/2\mathbf{Z}$, $v \mapsto \langle v, v\rangle \bmod 2$

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

is a group homomorphism thanks to the identity

$$\langle v+v', v+v'\rangle = \langle v,v\rangle + \langle v',v'\rangle + 2\langle v,v'\rangle. \tag{1}$$

We say L is *even* if this homomorphism is trivial, that is, if $\langle v,v\rangle \in 2\mathbf{Z}$ for all $v \in L$, or equivalently if all diagonal entries of G are even; else we say L is *odd*. If L is odd then the kernel of our homomorphism is an index-2 sublattice of L that consists of all lattice vectors of even norm and is thus called the *even sublattice* of L.

If L is integral and $\operatorname{disc} L$ is odd then the homomorphism $v \mapsto \langle v,v\rangle \bmod 2$ is represented by a unique coset C_L of $2L$ in L, meaning that for $c \in L$ we have $c \in C_L$ if and only if

$$\langle v,v\rangle \equiv \langle c,v\rangle \bmod 2 \tag{2}$$

for all $v \in L$. For example, $C_L = 2L$ if and only if L is even, and if $L = \mathbf{Z}^r$ (the lattice with Gram matrix I_r, the $r \times r$ identity matrix) then C_L consists of the vectors all of whose coordinates are odd. (The coset C_L is called the "canonical class" in [Serre 1973, Chapter V], while [Conway–Sloane 1999] uses the name "shadow of L" for the translate $\frac{1}{2}C_L$ of L in $L_{\mathbf{R}}$. For example, L is even if and only if L is its own shadow.) For $c, c' \in C_L$ we can then write $c' = c + 2v$ for some $v \in L$, and deduce

$$\langle c',c'\rangle = \langle c,c\rangle + 4(\langle c,v\rangle + \langle v,v\rangle) \equiv \langle c,c\rangle \bmod 8; \tag{3}$$

Thus $\langle c,c\rangle \bmod 8$ is independent of the choice of $c \in C_L$ and is an invariant, call it $\iota(L)$, of integral lattices L of odd discriminant. For example, if L is even then $0 \in C_L$, so $\iota(L)$ is 0 mod 8; if $L = \mathbf{Z}^r$ then $\iota(L)$ is r mod 8, a generalization of the familiar fact that all odd squares are 1 mod 8.

A fundamental result states:

Theorem 1. *If L is an integral lattice with $\operatorname{disc} L = \pm 1$ then*

$$\iota(L) = r_+(L) - r_-(L). \tag{4}$$

In particular if L is an even lattice with $\operatorname{disc} L = \pm 1$ then $r_+(L) \equiv r_-(L) \bmod 8$.

Proof: See [Serre 1973, Chapter V, Theorem 2, Corollary 2]. □

We aim for our exposition to be mostly self-contained, but must quote this theorem without proof; we later reduce several other structural results (Lemma 2, Proposition 3, Lemma 4 and its Corollary, and Proposition 5) to Theorem 1, rather than citing sources such as [Conway–Sloane 1999, Chapter 15] for the classification of general quadratic forms over $\mathbf{Z}$.

2.1.3. *New lattices from old: scaling, finite-index sublattices, and direct sums.* If L is a lattice and $d \in \mathbf{R}$ then we obtain a new lattice $L[d]$ by scaling the pairing by d:

$$\langle v,v'\rangle_{L[d]} = d \cdot \langle v,v'\rangle_L. \tag{5}$$

Thus if G is a Gram matrix for L then $d \cdot G$ is a Gram matrix for $L[d]$. The lattice $L[d]$ has the same rank as L; if $\operatorname{disc} L \neq 0$ then the signatures are related by $r_\pm(L[d]) = r_\pm(L)$ if $d > 0$ and $r_\pm(L[d]) = r_\mp(L)$ if $d < 0$.

If $L_1 \subseteq L$ is a subgroup of finite index then L_1 is a lattice with $\operatorname{rk} L_1 = \operatorname{rk} L$, $r_\pm(L_1) = r_\pm(L)$, and

$$\operatorname{disc} L_1 = [L : L_1]^2 \operatorname{disc} L. \tag{6}$$

Note that if $d \in \mathbf{Z}$ then the finite-index sublattice $d \cdot L$ is $L[d^2]$, not $L[d]$ (unless $d^2 = d$ or $L = \{0\}$).

If L_i $(1 \le i \le k)$ are lattices then the direct sum $\Lambda = \oplus_{i=1}^k L_i$ is a lattice of rank $\sum_{i=1}^k \operatorname{rk} L_i$, with the pairing

$$\langle (v_1, \ldots, v_k), (v_1', \ldots, v_k') \rangle = \sum_{i=1}^k \langle v_i \, , v_i' \rangle. \tag{7}$$

For example $\mathbf{Z}^k$ is the direct sum of k copies of $\mathbf{Z}$ (with the standard pairing $\langle a, a' \rangle = aa'$ on $\mathbf{Z}$). For any L_i, the direct sum Λ has signature $r_\pm(\Lambda) = \sum_{i=1}^k r_\pm(L_i)$; it is rational (resp. integral, even) if and only if the L_i are all rational (integral, even). If G_i are Gram matrices for the L_i then the block-diagonal matrix with diagonal blocks $G_1, \ldots, G_k$ is a Gram matrix for Λ. In particular, $\operatorname{disc}(\Lambda) = \prod_{i=1}^k \operatorname{disc} L_i$, so Λ is nondegenerate if and only if each L_i is.

2.1.4. *The dual lattice and discriminant group.* If L is nondegenerate then L has a *dual lattice* L^* which is also nondegenerate, defined by

$$L^* := \{v^* \in L_{\mathbf{R}} \mid \forall v \in L, \langle v^*, v \rangle \in \mathbf{Z}\}. \tag{8}$$

A $\mathbf{Z}$-basis $B = (e_1, \ldots, e_r)$ for L determines a dual $\mathbf{Z}$-basis $B^* = (e_1^*, \ldots, e_r^*)$ for L^*, characterized by $\langle e_i \, , e_j^* \rangle = \delta_{ij}$, and satisfying $G_{B^*} = G_B^{-1}$. It follows that $\operatorname{disc} L^* = (\operatorname{disc} L)^{-1}$, and also $B^{**} = B$, whence $L^{**} = L$. Also, the dual of a direct sum $\oplus_{i=1}^k L_i$ is the direct sum $\oplus_{i=1}^k L_i^*$ of the duals.

The dual lattice L^* is rational if and only if L is rational (in which case $L^* \subset L \otimes_{\mathbf{Z}} \mathbf{Q}$), and contains L if and only if L is integral, in which case $|\operatorname{disc} L| = [L^* : L]$. In this case we call the quotient group $\Delta_L := L^*/L$ the *discriminant group* of L; other names are "dual quotient group" and "glue group" [Conway–Sloane 1999, p. 48 and p. 100]. The pairing $\langle \cdot, \cdot \rangle : L^* \times L^* \to \mathbf{Q}$ descends to a perfect symmetric pairing $(\cdot, \cdot) : \Delta_L \times \Delta_L \to \mathbf{Q}/\mathbf{Z}$, which gives a yet finer invariant of L than the structure of Δ_L as an abelian group. Moreover, if L is even then we have a map $q_L : \Delta_L \to \mathbf{Q}/2\mathbf{Z}$ that takes each coset $v^* + L$ to $\langle v^*, v^* \rangle \bmod 2\mathbf{Z}$; the identity (1) shows that q_L is well-defined, and lets us recover the pairing $(\cdot, \cdot)$ from q_L. Our first result (Lemma 2) will determine the structure of the pairing and of q_L for any positive-definite even lattice L of rank $2 \bmod 8$ and prime discriminant $p \equiv -1 \bmod 4$, including our case of rank 18 and $p = 163$.

2.2. **Direct sums and gluing.** Suppose L is a nondegenerate integral lattice, with discriminant group Δ_L. If L is a finite-index sublattice of some integral lattice L' then $L \subseteq L' \subseteq (L')^* \subseteq L^*$, so L' is intermediate between L and L^*, and thus corresponds to some subgroup of $L^*/L = \Delta_L$. For a subgroup $H \subseteq \Delta_L$, the preimage of H in L^* is integral if and only if H is *isotropic* for the pairing $(\cdot, \cdot)$, meaning that $(c, c') = 0$ for all $c, c' \in H$. If L is even then the preimage of H is also even if and only if H is isotropic for q_L, meaning that $q_L(c) = 0$ for all $c \in H$; this is a stronger condition than isotropy for $(\cdot, \cdot)$.

This use of isotropic subgroups of Δ_L is a common construction of integral or even lattices, particularly when L is a direct sum. Suppose L_i $(1 \le i \le k)$ are nondegenerate lattices, and let Λ be their direct sum $\oplus_{i=1}^k L_i$. If each L_i, and thus also their direct sum Λ, is integral, then $\Delta_\Lambda = \oplus_{i=1}^k \Delta_{L_i}$; the pairing on Δ_Λ is the direct sum of the pairings on the Δ_{L_i}, and likewise for q_Λ when the L_i are all even. At least for $k = 2$, an integral lattice $\Lambda' \supset \Lambda$ corresponding to an isotropic $H \subset \Delta_\Lambda$ is said to be obtaind by "gluing" L_1 to L_2. (This is why [Conway–Sloane 1999, p.100] calls Δ_L the "glue group", and even ventures "self-glue" for the case $k = 1$.) Typically H has trivial intersection with both $\Delta_{L_1} \times \{0\}$ and $\{0\} \times \Delta_{L_2}$, and is thus the graph of some group isomorphism $i : H_1 \to H_2$ between subgroups of Δ_{L_1} and Δ_{L_2}. Then H is isotropic for $(\cdot,\cdot)$ if and only if i is an "anti-isomorphism" for the L_1 and L_2 pairings, i.e. $(ic, ic') = -(c, c')$ for all $c, c' \in H_1$; likewise H is isotropic for q_Λ if and only if $q(ic) = -q(c)$ for all $c \in H_1$.

2.3. **Positive-definite lattices: short vectors; roots and Weyl groups.** We henceforth assume, unless stated otherwise, that L is *positive-definite*, meaning that L is nondegenerate with $(r_+, r_-) = (\operatorname{rk} L, 0)$. Equivalent conditions are that $\langle v, v\rangle > 0$ for all nonzero $v \in L_{\mathbf{R}}$, and that G_B is positive-definite for any choice of $\mathbf{Z}$-basis B. In that case we can identify $L_{\mathbf{R}}$ with Euclidean space of dimension $\operatorname{rk} L$, and identify $\operatorname{disc} L$ with $\operatorname{Vol}(L_{\mathbf{R}}/L)^2$.

Since $L_{\mathbf{R}}$ is locally compact and L is a discrete subset, each ball $\langle v, v\rangle \le m$ contains only finitely many lattice vectors. (This is not a constructive argument; at the end of this section we outline how it can be made constructive for any L, and practical for the L and m that we need.) Denote by $L_{(m)}$ the finite set $\{v \in L : \langle v, v\rangle = m\}$, and by $\mathrm{N}_m(L)$ the size of this set; also write

$$L_{(\le m)} = \bigcup_{m' \le m} L_{(m')} = \{v \in L : \langle v, v\rangle \le m\}. \tag{9}$$

Note that if L is integral (resp. even) then $\mathrm{N}_m(L) = 0$ for all $m \notin \mathbf{Z}$ (resp. $m \notin 2\mathbf{Z}$). We next outline how the possible configurations $L_{(m)}$ of an integral lattice L can be described completely for $m = 1$ and $m = 2$.

The key ingredient is projection operators $\pi_\alpha : L_{\mathbf{R}} \to L_{\mathbf{R}}$, defined for any nonzero vector $\alpha \in L_{\mathbf{R}}$ by

$$\pi_\alpha(v) = v - \frac{\langle \alpha, v\rangle}{\langle \alpha, \alpha\rangle}\alpha. \tag{10}$$

This map projects any $v \in L_{\mathbf{R}}$ to the hyperplane $\alpha^\perp$ orthogonal to α. If L is integral and $\alpha \in L_{(1)}$ then (10) simplifies to $\pi_\alpha(v) = v - \langle \alpha, v\rangle\alpha$, and we see that $\pi_\alpha(v) \in L$ for all $v \in L$, so we have written L as the direct sum of $\mathbf{Z}\alpha$ with the lattice $L \cap \alpha^\perp$ of rank $\operatorname{rk}(L) - 1$. Repeating this procedure we write L uniquely as $\mathbf{Z}^k \oplus L_1$ where $\mathbf{Z}^k$ is generated by $L_{(1)}$ (so $k = \frac{1}{2}\mathrm{N}_1(L)$) and L_1 has no vectors of norm 1.

The case of $\alpha \in L_{(2)}$ is more interesting. Such α are called roots of L, and their $\mathbf{Z}$-span is the *root lattice* $R(L)$ of L. If α is a root, then π_α does not generally take L to L, but the reflection operator

$$s_\alpha(v) = (2\pi_\alpha - 1)v = v - 2\frac{\langle \alpha, v\rangle}{\langle \alpha, \alpha\rangle}\alpha \tag{11}$$

does, because when $\langle \alpha, \alpha\rangle = 2$ the formula (11) simplifies to $s_\alpha(v) = v - \langle \alpha, v\rangle\alpha$. These reflections generate a subgroup of $\operatorname{Aut}(L)$, called the *Weyl group* $W_L = W_{R(L)}$, which is a normal subgroup of $\operatorname{Aut}(L)$ that acts trivially on the orthogonal complement of $R(L)$ and on L^*/L. It is well-known (see any text on Lie algebras or on Euclidean reflection groups) that $R(L)$ decomposes uniquely as the direct sum $\oplus_i R_i$ of simple root lattices, with each simple root lattice appearing on the following list:

- A_n, which is the intersection of $\mathbf{Z}^{n+1}$ with the hyperplane $\sum_{i=1}^{n+1} a_i = 0$ of $\mathbf{Z}^{n+1}$, and has discriminant $n+1$;
- the "checkerboard lattice" D_n $(n \geq 4)$, which is the even sublattice of $\mathbf{Z}^n$, i.e., the index-2 sublattice $\sum_{i=1}^{n} a_i \equiv 0 \bmod 2$, and thus has discriminant $[\mathbf{Z}^n : D_n]^2 = 4$; and
- the exceptional lattices E_n $(n = 6, 7, 8)$, which have discriminant $9-n$, and are not contained in any $\mathbf{Z}^r$, but can be constructed in various other ways, for example as index-2 superlattices of $A_1 \oplus A_5$, $A_1 \oplus D_6$, and D_8 (in other words, by gluing A_1 to A_5 or D_6 and by self-gluing D_8).

Moreover, $L_{(2)}$ is the disjoint union of the $(R_i)_{(2)}$, and $W_{R(L)} = \prod_i W_{R_i}$. We summarize the main invariants of these root systems in the following table.

R	A_n	D_n	E_6	E_7	E_8
$\mathrm{disc}(R)$	$n+1$	4	3	2	1
$\mathrm{N}_2(R)$	$n(n+1)$	$2n(n-1)$	72	126	240
$\#W_R$	$(n+1)!$	$2^{n-1}n!$	$2\cdot5\cdot6\cdot8\cdot9\cdot12 = 51840$	$56\,\#W_{E_6} = 2903040$	$240\,\#W_{E_7} = 696729600$

Table 1: Root numbers $\mathrm{N}_2(R)$ and orders of Weyl groups W_R of simple root lattices R

Furthermore, we can choose a *base* $B = (e_1, \ldots, e_r)$ of $R(L)$, which is a basis consisting of roots (the "simple roots") such that $\langle e_i, e_j\rangle \leq 0$ for all i, j with $i \neq j$. All such B are equivalent up to permutation and the action of $W_{R(L)}$. The cone generated by the dual basis B^* is a fundamental domain for the action of $W_{R(L)}$ on $R(L) \otimes_{\mathbf{Z}} \mathbf{R}$; that is, the $W_{R(L)}$-orbit of every $v \in R(L) \otimes_{\mathbf{Z}} \mathbf{R}$ contains a unique nonnegative combination of dual basis vectors (equivalently: a unique v_0 such that $\langle v_0, e_i\rangle \geq 0$ for each i). For example, if $R = A_n$ then W_R consists of the permutations of the $\mathbf{Z}^{n+1}$ coordinates; we may take $e_i = u_i - u_{i+1}$ (where the u_i are the standard unit vectors for $\mathbf{Z}^{n+1}$), and then the fundamental domain consists of all vectors $(a_1, \ldots, a_{n+1})$ with $\sum_i a_i = 0$ and $a_1 \leq a_2 \leq \ldots \leq a_{n+1}$. The inner products $\langle e_i^*, e_j^*\rangle$ are all nonnegative, and vanish only for e_i, e_j in different components of $R(L)$.

Note that L may contain vectors in the $\mathbf{Q}$-span of $R(L)$ that are not themselves in $R(L)$. We denote by $R^+(L)$ the "saturation" $L \cap (R(L) \otimes_{\mathbf{Z}} \mathbf{Q})$ of $R(L)$. For example, D_{16} together with the vector $\frac{1}{2}\sum_{i=1}^{16} u_i$ generates an even lattice L of discriminant 1 with $R(L) = D_{16}$ contained with index 2 in $R^+(L) = L$. The finite quotient group $R^+(L)/R(L)$ will figure in the dictionary between lattices and elliptic fibrations (§2.4), where $R^+(L)/R(L)$ appears as the torsion subgroup of the group of sections of the corresponding elliptic fibration.

No such classification is known or expected for any nonempty $L_{(m)}$ with $m > 2$ (including $L_{(4)}$ for an even lattice L).

Finally, as promised earlier we address the computation of sets $L_{(\leq m)}$ and thus also $L_{(m)}$. Let G be the Gram matrix associated to the $\mathbf{Z}$-basis $B = (e_1, \ldots, e_r)$ for L, and write $v = \sum_i a_i e_i$; then $\langle v, v\rangle = a^{\mathsf{T}} G a$, so we seek vectors $a \in \mathbf{Z}^r$ such that $a^{\mathsf{T}} G a \leq m$. Letting $G^{1/2}$ be the positive-definite square root of G, this gives

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

$\langle G^{1/2}a, G^{1/2}a\rangle \leq m$, so $G^{1/2}a$ has length at most $m^{1/2}$, whence

$$\langle a, a\rangle \leq \left(\left\|G^{-1/2}\right\|_2 m^{1/2}\right)^2 = \left\|G^{-1}\right\|_2 m. \tag{12}$$

This bound depends on the choice of basis B, and the computational problem of finding short vectors becomes notoriously intractable for lattices of large rank. Fortunately the ranks we need (at most 20 or so) are well within the tractable range. For $m \leq 4$ we obtain the complete list for any of our lattices in a fraction of a second in GP [PARI 2025] using the function `qfminim`, which applies a technique such as LLL to make G^{-1} manageably small and then applies the algorithm of [Fincke–Pohst 1985] to find all $a \in \mathbf{Z}^r$ that solve $a^{\mathsf{T}}Ga \leq m$ [PARI doc]. In particular, the determination of short vectors is not a computational obstruction to finding $R(L)$ and decomposing it as a direct sum of simple root lattices.

2.4. **Connection with elliptic surfaces.** In this paper we need elliptic surfaces only for motivation, in particular to motivate our interest in the special case of discriminant 163. Thus we give few details, limiting ourselves to elliptic fibrations of K3 surfaces in characteristic zero and reciting only a few relevant facts. For a full exposition of the theory, see [Schütt–Shioda 2019], in particular Chapter 6 for elliptic surfaces in general and Chapter 11 for K3 surfaces. Also, [Schütt–Shioda 2019, Chapter 1] treats lattices from the point of view of their appearance in the algebraic geometry of elliptic surfaces.

For an algebraic K3 surface X, the Néron–Severi group $\mathrm{NS}(X)$ together with the intersection pairing is a nondegenerate even lattice, with $r_+(\mathrm{NS}(X)) = 1$ by the index theorem. In characteristic zero, the Picard number $\rho = \mathrm{rk}(\mathrm{NS}(X))$ is at most 20. If $\rho = 20$ and X together with all of $\mathrm{NS}(X)$ is defined over $\mathbf{Q}$ then $\mathrm{disc}(\mathrm{NS}(X))$ is one of the 13 negative discriminants $d = -3$, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163 of class number 1; each of those is possible, for a surface $X_{|d|}$ that is unique except for twists of X_3, X_4 [Schütt 2010].

An *elliptic fibration* of a K3 surface X/k is a rational map $t : X \to \mathbf{P}^1$ whose generic fiber is an elliptic curve. It is known that this means X has a birational model $E : y^2 = x^3 + a_4(t)x + a_6(t)$ where a_4, a_6 are polynomials of degree at most 8 and 12 respectively. The *Mordell–Weil group* of the fibration is the group of rational points of E considered as an elliptic curve over $k(t)$. Some explicit elliptic fibrations of X_{163} with interesting Mordell–Weil groups are given in [Elkies 2007, Elkies–Klagsbrun 2020].

An elliptic fibration determines a decomposition $\mathrm{NS}(X) = U \oplus L[-1]$, where U is generated by the classes of the zero-section and fiber and (with other generators) has Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ with $(r_+, r_-) = (1, 1)$. The lattice L, called the *frame* of the fibration in [Schütt–Shioda 2019, page 123, Def. 6.14] is positive-definite of rank $\rho - 2$. For d prime, the frame gives a bijection between elliptic fibrations of X_d and positive-definite lattices of rank 18 and discriminant d.

The simple components of the root lattice $R(L)$ correspond to the reducible fibers of the fibration, and determine their reduction types except for an ambiguity for A_1 (either I_2 or III) and A_2 (either I_3 or IV).

The *Tate-Shioda theorem* [Schütt–Shioda 2019, page 118, Theorem 6.5] canonically identifies the Mordell–Weil group of an elliptic fibration with $L/R(L)$. In particular the Mordell–Weil rank r_{MW} is $\mathrm{rk}\, L - \mathrm{rk}\, R(L)$ (so $18 - \mathrm{rk}\, R(L)$ for us), and the Mordell–Weil torsion group T_{MW} is $R^+(L)/R(L)$.

3. Gluing: L to M to N

In this section we determine the structure of (Δ_L, q_L) for each of our lattices L (Lemma 2), and use this to show via the gluing method that L can be obtained uniquely up to isomorphism as a hyperplane slice of a positive-definite even lattice M of rank 19 and discriminant 4 (Proposition 3). We then use the gluing method again to classify all such M (Proposition 5 and Table 2): there are 16, each realized uniquely up to isomorphism as the slice of a Niemeier lattice N orthogonal to a copy of D_5 in N (equivalently: in $R(N)$). This lets us state our main result (Theorem 6), which we prove in the next two sections.

3.1. **Determination of q_L.** Fix a prime $p = 4a - 1$ (in our application $p = 163$), and denote by $\chi_p(\cdot) : \mathbf{Z} \to \{0, \pm 1\}$ the quadratic Dirichlet character mod p. Let L_0 be the positive-definite even lattice of rank 2 and discriminant p with Gram matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2a \end{smallmatrix}\right)$. Then the dual lattice L_0^* has Gram matrix $p^{-1}\left(\begin{smallmatrix} 2 & -1 \\ -1 & 2a \end{smallmatrix}\right)$, and thus contains a vector v_0^* with $\langle v_0^*, v_0^* \rangle = 2/p$. Since the coset $v_0^* + L_0$ generates $L_0^*/L_0 \cong \mathbf{Z}/p\mathbf{Z}$, it follows that every $v^* \in L_0^* \backslash L_0$ has $\langle v^*, v^* \rangle = b/p$ for some $b \in 2\mathbf{Z}$ with $\chi_p(b) = \chi_p(2) = (-1)^a$. We prove more generally:

Lemma 2. *Let L be any even lattice of rank r of discriminant $\pm p$, with $r_+(L) - r_-(L) \equiv 2 \bmod 8$, and let $v^* \in L^*$ be any vector with $v^* \notin L$. Then $\langle v^*, v^* \rangle = b/p$ for some $b \in 2\mathbf{Z}$ with $\chi_p(b) = \chi_p(2) = (-1)^a$.*

In particular this applies to our lattices, which have $(r_+, r_-) = (18, 0)$.

Remark: In effect Lemma 2 states that the hypotheses on L determine the isomorphism class of q_L. Namely, the discriminant group Δ_L has order $\mathrm{disc}\, L = p$, so $\Delta_L \cong \mathbf{Z}/p\mathbf{Z}$; such a group has three choices of quadratic form q_L, corresponding to the three possible values $1, 0, -1$ of $\chi_p(b)$, and we claim that $\chi_p(b)$ must equal $\chi_p(2) = (-1)^a$. This is the first result that we choose to prove by reducing to Theorem 1 via gluing rather than citing a general classification resut such as those in [Conway–Sloane 1999, Chapter 15].

Proof: We first show that $b \in 2\mathbf{Z}$. Since $L^*/L \cong \mathbf{Z}/p\mathbf{Z}$, we have $pv^* \in L$, so $b = \langle pv^*, v^* \rangle \in \mathbf{Z}$ and $pb = \langle pv^*, pv^* \rangle \in 2\mathbf{Z}$, which together imply that b is an even integer. Moreover $b \not\equiv 0 \bmod p$, because if $p \mid b$ then $\langle v^*, v^* \rangle \in \mathbf{Z}$ which would make L^* an integral lattice — which is impossible because $\mathrm{disc}\, L^* = p^{-1} \notin \mathbf{Z}$. (Alternatively, if b were a multiple of p then the pairing $(\cdot, \cdot)$ on Δ_L would be degenerate.)

Assume for the sake of contradiction that $\chi_p(b) = -\chi_p(2) = \chi_p(-2)$. Then $b \equiv -2r^2 \bmod p$ for some integer r. We shall reach a contradiction by gluing L to L_0 to construct an even lattice L_1 of discriminant ± 1 with $r_+(L_1) - r_-(L_1) \not\equiv 0 \bmod 8$. Namely, L_1 is the following lattice intermediate between the orthogonal direct sum $L \oplus L_0$ and its dual $(L \oplus L_0)^* = L^* \oplus L_0^*$: it is generated by $L \oplus L_0$ together with (v^*, rv_0^*). Indeed $\langle (v^*, rv_0^*), (v^*, rv_0^*) \rangle \in 2\mathbf{Z}$ by construction, and $\langle (v^*, nv_0^*), w \rangle \in \mathbf{Z}$

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

for all $w \in L \oplus L_0$ because $(v^*, nv_0^*) \in (L \oplus L_0)^*$, so L_1 is an even lattice. Moreover, $\operatorname{disc} L_1 = \pm 1$ because

$$p^2 = \operatorname{disc}(L \oplus L_0) = [L_1 : (L \oplus L_0)]^2 \operatorname{disc} L_1 = p^2 \operatorname{disc} L_1, \tag{13}$$

and $r_+(L_1) - r_-(L_1) = r_+(L) + 2 - r_-(L) \equiv 4 \bmod 8$. This contradicts Theorem 1. □

3.2. **From L to M.** Henceforth we assume further that $p \equiv 3 \bmod 8$, as is still the case for our prime $p = 163$, and consider only positive-definite L.

Proposition 3. *Fix a positive integer $r \equiv 2 \bmod 8$. There is a bijection between: positive-definite even lattices L of rank r and discriminant p up to isomorphism; and ordered pairs (M, v^*) where M is a positive-definite even lattice of rank $r+1$ and discriminant 4, and $v^* \in M^*$ satisfies $\langle v^*, v^* \rangle = p/4$, up to isomorphism. This bijection associates to (M, v^*) the lattice*

$$L = \{v \in M : \langle v^*, v \rangle = 0\}. \tag{14}$$

Proof: Given (M, v^*), we first check that (14) gives a lattice that is even, positive-definite, and of rank r and discriminant p. The first two properties are inherited from M. Also L has rank r because it is the intersection of a lattice of rank $r+1$ with a rational hyperplane. To compute $\operatorname{disc} L$, consider $L \oplus \mathbf{Z}v^*$, a sublattice of M^*. The sum is direct, and the sublattice has rank $r+1$ and thus finite index. Hence we can write its discriminant as both

$$\operatorname{disc}(L \oplus \mathbf{Z}v^*) = \operatorname{disc}(L) \operatorname{disc}(\mathbf{Z}v^*) = \operatorname{disc}(L) \cdot \frac{p}{4} \tag{15}$$

and

$$\operatorname{disc}(L \oplus \mathbf{Z}v^*) = [M^* : (L \oplus \mathbf{Z}v^*)]^2 \operatorname{disc} M^* = [M^* : (L \oplus \mathbf{Z}v^*)]^2 \cdot \frac{1}{4}. \tag{16}$$

Hence $\operatorname{disc} L = p^{-1}[M^* : (L \oplus \mathbf{Z}v^*)]^2$. But the index $[M^* : (L \oplus \mathbf{Z}v^*)]$ is a factor of p because $L \oplus \mathbf{Z}v^*$ consists of all $w^* \in M^*$ such that $p \mid 4\langle v^*, w^* \rangle$. (This condition is clearly necessary, and if $\langle v^*, w^* \rangle = bp/4$ for some $b \in \mathbf{Z}$ then $w^* - bv^* \in L$.) The index cannot equal 1 because then L would be an integral lattice of fractional discriminant $1/p$. Therefore $[M^* : (L \oplus \mathbf{Z}v^*)] = p$, so $\operatorname{disc} L = p$ as claimed.

We reverse this construction to recover (M, v^*) from L. Let L_1 be the even lattice of rank 1 and discriminant $4p$, so $L_1 = \mathbf{Z}v_1$ with $\langle v_1, v_1 \rangle = 4p$. Then L_1^* contains the vector v_1/p of norm $4/p$. By Lemma 2, L^* contains v^* such that $\langle v^*, v^* \rangle \equiv -4/p \bmod 2\mathbf{Z}$. Hence we can glue L to L_1: let M be the even lattice generated by $L \oplus L_1$ and $(v^*, v_1/p)$, which contains $L \oplus L_1$ with index p and thus has discriminant 4 as desired. Moreover L is the slice of M orthogonal to the vector $v_1/4$ of norm $p/4$. Finally, v^* is unique up to translation by L, which does not change M, and changing v^* to $-v^*$, which still yields an isomorphic lattice via replacing v_1 by $-v_1$. □

3.3. **From M to N.** We next give two ways to classify M: as the even sublattice of an odd lattice $\overline{M}$ of rank 19 and discriminant 1 ("self-gluing" M), and as the slice of an even lattice N of rank 24 and discriminant 1 that is orthogonal to a copy of D_5 (gluing M to D_5).

Lemma 4. *Fix an odd integer $r > 0$. There is a bijection up to isomorphism between: positive-definite even lattices M of rank r with $M^*/M \cong \mathbf{Z}/4\mathbf{Z}$, and positive-definite lattices $\overline{M}$ of rank r and discriminant 1. This bijection associates to M the preimage of $2\mathbf{Z}/4\mathbf{Z}$ under the map $M^* \to M^*/M \overset{\cong}{\to} \mathbf{Z}/4\mathbf{Z}$; the inverse bijection associates to $\overline{M}$ its even sublattice $M = \{v \in \overline{M} : \langle v, v\rangle \equiv 0 \bmod 2\}$.*

Proof: Given M, choose $v^* \in M^*$ such that the coset $v^* + M$ generates M^*/M. Then $2v^* \notin M$, but $4v^* \in M$, so

$$\langle 2v^*, 2v^*\rangle = 4\langle v^*, v^*\rangle = \langle v^*, 4v^*\rangle \in \mathbf{Z}. \tag{17}$$

Hence $\overline{M}$ is an integral lattice with $[\overline{M} : M] = 2$, so $\operatorname{disc}\overline{M} = \operatorname{disc} M/2^2 = 1$. Thus $\overline{M}$ is odd since it has discriminant 1 and odd rank. Clearly M is the even sublattice of this $\overline{M}$. To go in the reverse direction, let $\overline{M}$ be a positive-definite lattice of rank r and discriminant 1, with even sublattice M and characteristic vector c. Then $\langle c, v\rangle \in 2\mathbf{Z}$ for all $v \in M$, so $c/2 \in M^*$. Clearly $2c \in M$; but $c \notin M$, because $\langle c, c\rangle$ is odd by Theorem 1. Hence the image of $c/2$ in M^*/M has order 4, whence $M^*/M \cong \mathbf{Z}/4\mathbf{Z}$ because $[M^* : M] = |\operatorname{disc} M| = 4$. □

Corollary: If M is positive-definite even lattice of odd rank r with $M^*/M \cong \mathbf{Z}/4\mathbf{Z}$ then $\langle v^*, v^*\rangle \in 2\mathbf{Z} + r/4$ for any dual vector $v^* \in M^*$ such that $v^* + M$ generates M^*/M.

Proof: We just saw that $2v^*$ is a characteristic vector of $\overline{M}$. Hence $4\langle v^*, v^*\rangle = \langle 2v^*, 2v^*\rangle \equiv r \bmod 8$. □

We can use this to find all possible M as long as the lattices $\overline{M}$ of rank r and discriminant 1 have all been classified; the record here, which long stood at 25, has recently been pushed [Allombert–Chenevier 2025, Chenevier–Taïbi 2026] to 28 and then to 29. For $r = 19$ there are 16 lattices, see [Conway–Sloane 1999, page 49, Table 2.2; and page 416, Table 16.7][1] or [OEIS 2026]. Alternatively, we can use the Corollary to simplify the hypotheses of the next Proposition, which is the source of the classification of discriminant-1 lattices of odd ranks $r \le 23$.

Proposition 5. *Fix odd integers r, r' such that $r + r' \equiv 0 \bmod 8$. Then there is a bijection up to isomorphism between: positive-definite even lattices M of rank r with $M^*/M \cong \mathbf{Z}/4\mathbf{Z}$, and pairs (N, N_0) where N is a positive-definite even lattice of rank $r + r'$, and $N_0 \subset N$ is a sublattice isomorphic with $D_{r'}$. The bijection takes (N, N_0) to the intersection of N with the orthogonal complement of N_0.*

Here we define $D_{r'}$ as the even sublattice of $\mathbf{Z}^{r'}$ even for $r' = 3$ (with $D_3 \cong A_3$) and $r' = 1$ (with $D_1 = 2\mathbf{Z} \cong \mathbf{Z}[4]$).

Proof: Given (N, N_0), let $M \subset N$ be the orthogonal complement of N_0. Then $M \oplus N_0$ contains N with index at most 4: the projection to $N_0 \oplus_{\mathbf{Z}} \mathbf{R}$ takes N to N_0^*, which contains N_0 with index 4. Since $\operatorname{disc} N = 1$ and $\operatorname{disc} N_0 = 4$ we find

$$4 \operatorname{disc} M = \operatorname{disc}(M \oplus N_0) = [N : (M \oplus N_0)]^2; \tag{18}$$

[1]Note that Table 16.7 lists only lattices L of discriminant 1 with $\mathrm{N}_1(L) = 0$. In rank 19 there are three such L. The 13 remaining lattices, which do have vectors of norm 1, can be recovered as $\mathbf{Z}^k \oplus L_1$ for some $k > 0$ and lattice L_1 of rank $19 - k$ that is listed earlier in the table.

since M is an even lattice of odd rank, it cannot have discriminant 1, so $[N : (M \oplus N_0)] = 4$ (whence the projection map $N \to N_0^*$ is surjective) and $\operatorname{disc} M = 4$. It also follows that N is obtained by gluing M to N_0: if $N/(M \oplus N_0)^*$ had nontrivial intersection with M^*/M or N_0^*/N_0 then M or N_0 would be contained in an even lattice of discriminant 1, which cannot exist because r and r' are odd.

To prove that this is a bijection, we must show that $M \oplus D_{r'}$ is contained in a lattice N of discriminant 1, which is unique up to an automorphism of (N, N_0) (with N_0 being the $D_{r'}$ factor of $M \oplus D_{r'}$). By the Corollary to Lemma 4, q_M takes each generator of Δ_M to $r/4$. Either by applying the same Lemma to $D_{r'}$, or by direct computation ($\Delta_{D_{r'}}$ is generated by the vector each of whose r coordinates is 1/2), we see that $q_{D_{r'}}$ takes each generator to $r'/4$. By assumption $(r/4) + (r'/4) \in 2\mathbf{Z}$, so M and $D_{r'}$ have anti-isomorphic discriminant groups. There are two choices of anti-isomorphism, but they are equivalent under the automorphism $(-1_M, 1_{D_{r'}})$. Hence N exists and is unique up to automorphism. □

This is useful if $r + r'$ is small enough that the positive-definite even lattices N of rank $r + r'$ can be classified. At present this means $r + r' \le 24$. In our setting $r = 19$, so we take $r' = 5$ and find that N is one of the *Niemeier lattices*, the 24 positive-definite even lattices of rank 24 and discriminant 1 (see e.g. [Venkov 1978] ≅ [Conway–Sloane 1999, Chapter 18]). Because D_5 is a root lattice, an embedding $D_5 \to N$ must send D_5 to one of the simple factors of $R(N)$, which must be either D_n (some $n \ge 5$) or one of the three E_n. There are 13 choices of N, leading to the following table:

$R(M)$	D_{19}	$D_{11}E_8$	$A_3E_8^2$	A_3D_{16}	D_7D_{12}	$D_5E_7^2$	A_1A_{17}	$A_1D_{10}E_7$
$R^+(M)/R(M)$	$\{0\}$	$\{0\}$	$\{0\}$	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/2\mathbf{Z}$
$R(N)$	D_{24}	$D_{16}E_8$	E_8^3	$D_{16}E_8$	D_{12}^2	$D_{10}E_7^2$	$A_{17}E_7$	$D_{10}E_7^2$
$[\mathrm{Aut}(M) : W_{R(M)}]$	2	2	4	2	2	4	4	2

$R(M)$	$A_{15}D_4$	$A_3D_8^2$	E_6^3	$A_1^2A_{11}E_6$	$A_{11}D_7$	D_6^3	A_9^2	$A_7^2D_5$
$R^+(M)/R(M)$	$\mathbf{Z}/4\mathbf{Z}$	$(\mathbf{Z}/2\mathbf{Z})^2$	$\mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/6\mathbf{Z}$	$\mathbf{Z}/4\mathbf{Z}$	$(\mathbf{Z}/2\mathbf{Z})^2$	$\mathbf{Z}/5\mathbf{Z}$	$\mathbf{Z}/8\mathbf{Z}$
$R(N)$	$A_{15}D_9$	D_8^3	E_6^4	$A_{11}D_7E_6$	$A_{11}D_7E_6$	D_6^4	$A_9^2D_6$	$A_7^2D_5^2$
$[\mathrm{Aut}(M) : W_{R(M)}]$	4	4	12	4	2	12	8	4

Table 2: The 16 even lattices M and the associated Niemeier lattices N

Each of the three lattices N with $R(N) = D_{16}E_8$, $D_{10}E_7^2$, and $A_{11}D_7E_6$ appears twice because D_5 embeds in $R(N)$ in two inequivalent ways. It is known that if a simple root lattice R appears several times in N then all these copies are equivalent under $\mathrm{Aut}(N)$, and if R accommodates D_5 then the image is unique up to the action of the Weyl group $W_R \subset \mathrm{Aut}(N)$; but each of D_{16} and E_8, D_{10} and E_7, and D_7 and E_6 accommodates a copy of D_5. We shall also need the index $[\operatorname{Aut} M : W_M] = [\operatorname{Aut} M : W_{R(M)}]$ of the Weyl group of each M in its full automorphism group, and thus tabulate these indices in the last row of Table 2.

Having found the 16 lattices in Table 2, we check that the list is complete using the Minkowski–Siegel mass formula, as was done in [Conway–Sloane 1982] for the Niemeier lattices themselves (see also [Conway–Sloane 1982, page 413, Table 16.6]). Denote by Mass_4 the total mass $\sum_M 1/\#(\mathrm{Aut}(M))$ of positive-definite even lattices of rank 19 and discriminant 4, which by Lemma 4 is also the total mass of positive-definite even lattices of rank 19 and discriminant 1. For the lattices in Table 2, we compute

(19)
$$\sum_M \frac{1}{\#(\mathrm{Aut}(M))} = \frac{8003636403977}{77489135679822039613440000} = \frac{73 \cdot 691 \cdot 3617 \cdot 43867}{2^{35}\, 3^{13}\, 5^4\, 7^2\, 11 \cdot 13 \cdot 17 \cdot 19}$$

which is numerically $1.032872\ldots \cdot 10^{-13}$. The factorization is already promising because we recognize the numerators of the Bernoulli numbers $B_{12} = -691/2730$, $B_{16} = -3617/2730$, and $B_{18} = 43867/798$. If (19) agrees with the Minkowski–Siegel formula for Mass_4 then our list is complete because any further M would make the sum larger.

We can now proceed in several ways. For lattices of discriminant 1, the masses are tabulated in [Conway–Sloane 1999, pages 410–411, Table 16.2]; the rank-19 value agrees with (19). We can also ask Sage [Sage 2023] for the mass of our genus of quadatic forms; happily it also agrees with (19). Finally, we can check the Minkowski–Siegel mass formula directly. Writing

$$\sum_M \frac{1}{\#(\mathrm{Aut}\, M)} = Z_4 \prod_{k=1}^{9} |B_{2k}|\,, \tag{20}$$

we find that the complementary factor Z_4 is

$$Z_4 = \frac{73}{27179089920} = \frac{2^9 - 1}{2^{19}\, 9!}, \tag{21}$$

as predicted.

3.4. **Statement of main result.** It remains to find all dual vectors of norm 163/4 for each of the 16 possible M, up to $\mathrm{Aut}\, M$. We do this in the next section (§4), finding:

Theorem 6. *There are* 167889 *isomorphism classes of positive-definite even lattices of rank* 18 *and discriminant* 163*. Their distribution by* M *and by Mordell–Weil torsion and rank is given by Tables 5 and 6 in §6.*

4. The main computation

We do the following for each M. We seek all $v^* \in M^*$ of norm 163/4, up to the action of $\mathrm{Aut}(M)$. According to Table 2, the quotient of $\mathrm{Aut}(M)$ by its Weyl group W_M is small — at most 12, usually 2 or 4. Choose for each $g \in \mathrm{Aut}(M)/W_M$ a lift $\bar{g} \in \mathrm{Aut}(M)$.

Choose a base B for $R(M)$, let $B^* = (e_1^*, \ldots, e_r^*)$ be the dual basis, and let π be the projection from M^* to $R(M) \otimes \mathbf{Q}$. Let $\mathcal{D}$ be the preimage under π of the nonnegative linear combinations of B^*; this is a fundamental domain for the action of W_M on $M_{\mathbf{R}}$. We first find all $v^* \in M^* \cap \mathcal{D}$ with $\langle v^*, v^* \rangle = 163/4$, then collect them into orbits under $\mathrm{Aut}(M)/W_M$ and extract a representative from each orbit.

Recall that $(R(M))^*$ is the $\mathbf{Z}$-span of B^*. Denote by Λ the $\mathbf{Z}$-span of πM^* and $(R(M))^*$. Then Λ contains B^* with finite index. If $v^* \in M^*$ has norm 163/4 then $\pi v^* \in \Lambda$ is a vector of norm at most 163/4. For each coset C of $(R(M))^*$ in Λ it is easy to find all $w \in C \cap \mathcal{D}$ with $\langle w, w \rangle \le 163/4$. Indeed choose minimal $a_i \ge 0$ such that $C \ni \sum_i a_i e_i^*$; then $C \cap \mathcal{D}$ consists of all $\sum_i a_i' e_i^*$ with each $a_i' = a_i + b_i$ for some integer $b_i \ge 0$. Since $\langle e_i^*, e_j^* \rangle \ge 0$ for all i, j, the norm of $\sum_i a_i' e_i^*$ is an increasing function of each a_i'. This lets us list all solutions in lexicographic order without any wasted effort.

For each w that we find, we readily find its preimages, if any, of norm $163/4$ in M^*. In our setting $M/R(M)$ has rank at most 1 so we need only solve for one missing component and check whether the resulting v^* actually lands in M^*; in general the technique still works with reasonable efficiency as long as the rank of $M/R(M)$ is not too large: we must search for small lattice points in a space of dimension $\operatorname{rk} M - \operatorname{rk} R(M)$.

Finally apply each $\bar{g}$ to v^*, and use the reflections $s_{e_i} \in W_M$ to bring $\bar{g}v^*$ into $\mathcal{D}$. Output v^* if it is lexicographically minimal among all the resulting vectors. At the end, sort the vectors v^* and remove duplicates to get the desired list.

This computation took at most half an hour for each M, and usually much less.

5. Verifying correctness

Even this relatively simple calculation can be prone to errors and bugs. Here we describe some "sanity checks" that we used for reassurance that we were on the right track, followed by an independent verification that our list of 167889 lattices is correct.

5.1. **Smaller $p \equiv 3 \bmod 8$.** Since the technique applies to all prime $p \equiv 3 \bmod 8$, we did the calculation for some smaller such p for which we already knew the answer, from the literature or by constructing the 2-neighbor graph. When the answers finally matched, we redid it for the remaining such $p < 163$. These still agreed with all the values we had already calculated (through $p = 83$, and thus including $p = 67$ which corresponds to the second-to-last K3 surface with maximal-rank Néron–Severi group all defined over $\mathbf{Q}$); we also obtained several further counts:

D	3	11	19	43	59	67	83	107	131	139	163
H	6	33	111	998	2751	4421	9657	26658	62916	82077	167889

Table 3: Counts of even lattices L of rank 18 and prime discriminant $p = 8k + 3 \leq 163$

All but the first few of these were not previously published.

5.2. **The mass formula.** The mass formula again gives a powerful check on the computation that we then upgrade to a proof of completeness. Here there are far too many lattices L to compute each $\#\operatorname{Aut}(L)$ by hand, so we must rely on qfauto [PARI doc] or some other efficiently implemented method to automatically find each $\#\mathrm{Aut}(L)$.

Besides the large number of lattices, we face a new difficulty that did not arise for computing $\#\mathrm{Aut}(M)$ for each of the 16 lattices M in Table 2. GP's functions qfauto and qfisom find lattice automorphisms and isomorphisms using algorithms of [Plesken–Souvignier 1997], which reduce automorphisms and isomorphisms of lattices to automorphisms and isomorphisms of the lattices' configurations of short vectors. The "short vectors" are all lattice vectors v with $\langle v, v\rangle \leq m_0$, for any m_0 large enough that these vectors generate the lattice. For the 16 lattices M, we could always take $m_0 = 4$ (and even $m_0 = 2$ suffices for the first three lattices in Table 2, which are the root lattics D_{19}, $D_{11}E_8$, and $A_3E_8^2$). For each M, the ball

$\langle v,v\rangle \le 4$ contains at most 48178 nonzero lattice vectors; qfauto computes $\#\mathrm{Aut}\,M$ in a matter of seconds. Most of the 167889 lattices L are likewise generated by their vectors of norm at most 4, whose count can be no larger than for the lattice $M \supset L$. It would be reasonable to spend a few seconds on each of them, computing all their mass contributions $1/\#\mathrm{Aut}(L)$ in a matter of days. But 3548 of those L's are not generated by their vectors of norm at most 4, and so require $m_0 \ge 6$; and of those, 588 require $m_0 \ge 8$, which is already impractical. There are even two L that require $m_0 \ge 82$: the lattices $L = L_0 \oplus \Lambda$, where L_0 is the lattice with Gram matrix $\binom{2\ \ 1}{1\ \ 82}$, and Λ is one of the two even lattices of rank 16 and discriminant 1. For those L it is utterly infeasible to just store all lattice vectors with $\langle v,v\rangle \le 82$ (there are over $5\cdot 10^{14}$), let alone compute their configuration's automorphisms. To be sure these particular $\mathrm{Aut}(L)$ are not hard to determine (in each case $\mathrm{Aut}\,L = \mathrm{Aut}\,L_0 \times \mathrm{Aut}\,\Lambda$), but we would not want to compute hundreds of such automorphism counts by hand, and could have little confidence that they are all correct.

Fortunately there is a shortcut to this computation and many like it: apply the Plesken–Souvignier algorithm not to L but to its dual lattice L^*, scaled by 163 to make it integral because qfauto requires an integer Gram matrix. The lattice $L^*[163]$ has the same automorphism group as L, but typically is characterized by a much smaller configuration of short vectors. We can always take for m_0 the largest diagonal entry of a Gram matrix. For each L, we computed an LLL-reduced Gram matrix for L^*, and chose as our m_0 its largest diagonal entry, which was about 1.9 on average. We found that there are on average fewer than 800 vectors of norm at most m_0, compared with 8000+ vectors of norm at most 4 for L. (The largest m_0 needed is 4, seen for $L = L_0 \oplus \Lambda$ where $[\Lambda : D_{16}] = 2$; even here L^* has only 96154 nonzero short vectors.) Moreover the short vectors of L^* or $L^*[163]$ typically have many more $\langle v,v\rangle$ and $\langle v,v'\rangle$ values than the short vectors of L. This suggests that it should be much more efficient to apply qfauto to $L^*[163]$ rather than L for every L in our list, not just the small fraction of lattices not generated by their vectors of norm 2 and 4.

Done this way, the mass calculation took under half an hour, finding

$$\sum_L \frac{1}{\#(\mathrm{Aut}(L))} = \frac{4192308179228267199358 7}{188813683430365593600 00} = \frac{47\cdot 691\cdot 1213\cdot 3617\cdot 294217150811}{2^{32}\,3^{10}\,5^4\,7^2\,11\cdot 13\cdot 17} \tag{22}$$

which is numerically 2.22034+. Again the factorization is promising because we recognize the numerators of the Bernoulli numbers $B_{12} = -691/2730$ and $B_{16} = -3617/2730$.

As with the list of lattices M, we have several ways to conclude. Sage computes the Minkowski–Siegel mass, which happily agrees with (22). Alternatively we can start by writing

$$\sum_L \frac{1}{\#(\mathrm{Aut}(L))} = Z \prod_{k=1}^{8} |B_{2k}|\,, \tag{23}$$

finding that the complementary factor Z is

$$Z = \frac{16773613984885921}{5284823040} = \frac{47\cdot 1213\cdot 294217150811}{2^{24}\,3^2\,5\cdot 7}; \tag{24}$$

so it remains to verify that

$$L(9,\chi_{163}) = \frac{\pi^9}{163^{17/2}} \cdot \frac{2^2\, 47 \cdot 1213 \cdot 294217150811}{3^2\, 5 \cdot 7}\,. \tag{25}$$

(The exponent of 26 in the factor 2^{26} of the ratio between Z and (25) arises as $(3/2)\,\mathrm{rk}(L)-1$.) We can compute $L(9,\chi_{163})$ to high precision, for example by telling `GP` "`lfun(x^2+163, 9) / zeta(9)`", which uses the identity $\zeta_K(s) = \zeta(s)L(s,\chi_{163})$ where K is the imaginary quadratic field $\mathbf{Q}(\sqrt{-163})$. The agreement between the resulting value 0.99799944+ and (25) is already enough to prove (25) if we know *a priori* that $9!\ 163^{17/2}L(9,\chi_{163})/\pi^9 \in \mathbf{Z}$. Alternatively, we can use the closed form

$$L(9,\chi_{163}) = -\frac{2^8\pi^9}{9!\sqrt{163}} \sum_{a=1}^{162} \chi_{163}(a) B_9(a), \tag{26}$$

where B_9 is the 9th Bernoulli polynomial

$$B_9(x) = \text{“}[x+B]^9\text{”} = \sum_{k=0}^{9} \binom{9}{k} B_{9-k}x^k = x^9 - \frac{9}{2}x^8 + 6x^7 - \frac{21}{5}x^5 + 2x^3 - \frac{3}{10}x. \tag{27}$$

We calculate that the sum in (26) is

$$-\frac{301925051727946578}{498311414318121121} = -\frac{2\cdot 3^2\, 47 \cdot 1213 \cdot 294217150811}{163^8}, \tag{28}$$

which gives yet another confirmation that we have the correct mass.

5.3. **Lattice signatures.** We have one final difficulty to overcome: we must prove that all our lattices L are distinct. If some L were to appear more than once in our list, then L would contribute more than its share to our mass calculation, meaning that some mass — and thus some other lattice(s) — was missing. To be sure it seems most unlikely that the apparent extra mass and the actual missing mass would exactly match, and in any case all our L should be distinct by our calculation. But we want a technique that can prove Theorem 6 and similar results using just a list of Gram matrices, without having to check and rerun the algorithm used to find them in the first place, and indeed independent of how the list was obtained. The mass calculation satisfies this criterion; we shall prove under the same constraint that our 167889 lattices L are all pairwise distinct.

In principle such a check was already required for proving completeness of the list of Niemeier lattices and the list (Table 2) of lattices M using the mass formula. But in each of those cases we already learn enough in the course of the mass computation to distinguish all the lattices, for instance because in each list no two root lattices $R(L)$ coincide, nor do any two automorphism counts $\#\,\mathrm{Aut}(L)$. Even without this information, there are few enough lattices in each list that we might simply check each pair. But this would be a huge computation for our 167889 lattices; we estimate that the time to check lattice isomorphism for each of $1.4\cdot 10^{10}$ pairs would be several CPU decades.

We could still check only pairs $\{L, L'\}$ with $R(L) = R(L')$. There are 1402 root lattices $R(L)$ that appear (see (6.4)), so this greatly reduces the number of `qfisom` calls, but not enough: we still count $66320273 > 6.6\cdot 10^7$ pairs. However, this points in the right direction. For each L we compute what we call a "signature": a few invariants that can be evaluated quickly and together come close to distinguishing all 167889 lattices from each other. The signature need only be computed once per L, and need not be a complete invariant, only close enough that few matching pairs remain. We used a signature with the following components:

- The counts $\mathrm{N}_2(L)$ and $\mathrm{N}_4(L)$ of vectors $v \in L$ with $\langle v, v\rangle = 2$ (roots) and $\langle v, v\rangle = 4$. These vectors are computed quickly by the GP function `qfminim`.
- The structure of $R(L)$, that is, the simple factors of $R(L)$ with multiplicity. Having computed all $\mathrm{N}_2(L)$ roots α, the simple factors of $R(L)$ correspond to connected components of the graph whose vertices are the roots and edges are pairs $\{\alpha, \alpha'\}$ of distinct roots such that $\langle \alpha, \alpha'\rangle \neq 0$. The type A_n, D_n, or E_n of each irreducible component is determined by its number of roots and the rank of the subgroup of L that they span, see Table 1.
- The structure of the torsion group $R^+(L)/R(L)$. This amounts to the Smith normal form of a matrix of a $\mathbf{Z}$-basis of $R(L)$

The connection with elliptic fibrations gives us an independent reason for computing the invariants $R(L)$ and $R^+(L)/R(L)$: as we noted earlier, they reflect the reducible fibers and torsion group of the elliptic fibration corresponding to L. Indeed that is the main reason to tabulate $R^+(L)/R(L)$, which does not contribute much to distinguishing between different L because $R^+(L) = R(L)$ for the vast majority (almost 98%) of lattices L.

We computed this signature $\sigma(L)$ for each of our 167889 lattices, sorted them by $\sigma(L)$, and collected together all L with the same $\sigma(L)$. This already distinguishes most L from each other: there are 156999 different signatures, with multiplicities distributed as follows.

μ	1	2	3	4	5	6	7	8	9	10	11	12	16
m_μ	147942	7965	623	345	41	55	11	10	3	1	1	1	1

Table 4: Counts m_μ of lattice signatures appearing with multiplicity μ

We check that $\sum_\mu \mu m_\mu = 167889$ as expected. The number of pairs $\{L, L'\}$ of lattices that we still had to distinguish is $\sum_\mu \binom{\mu}{2} m_\mu = 14044$. Again we did this using the trick of checking lattice isomorphism not of L and L' but of their duals, replacing each Gram matrix G by $163/G$ before calling `qfisom`. As expected, all pairs were distinct. This computation took under an hour, and completed the verification of Theorem 6 by checking that our list of Gram matrices represents 167889 different lattices and constitutes a full census of even positive-definite lattices of rank 18 and discriminant 163.

We conclude this section by listing some further components of a lattice signature that we did not use (there was little motivation to implement more invariants once we had reduced the calculation to under an hour) but might be of use in further such computations.

- Beyond $\mathrm{N}_2(L)$ and $\mathrm{N}_4(L)$, we already computed $\mathrm{N}_6(L)$, and it may even be worth taking the time to compute $\mathrm{N}_8(L)$. Note, though, that there are pairs of lattices that have the same theta series

$$\theta_L(q) = \sum_{m=0}^{\infty} N_{2m}(L) q^m = \sum_{v \in L} q^{\langle v,v\rangle/2}, \tag{29}$$

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

and thus cannot be distinguished by any number of N_m values. This already happens for some Niemeier lattices, and seems to also be the case for each of the largest batches of L in our list with the same $\sigma(L)$ (the $\mu \geq 10$ entries in Table 4).

- Likewise we can compute the smallest few norms of the scaled dual lattices $L^*[163]$. This, too, will not distinguish lattices with the same theta series, due to the functional equation relating θ_L with θ_{L^*}.

- We already computed the counts $\mathrm{N}_4(R^+(L))$ and $\mathrm{N}_6(R^+(L))$, which can distinguish between pairs of saturated root lattices that have the same $R(L)$ and $R^+(L)/R(L)$; we did not need these counts for our computation, but do include them in the shared data described in the last section (§7) of this paper.

- We can include $\#\operatorname{Aut}(L)$ in $\sigma(L)$: it is not as easy to compute as the other components of $\sigma(L)$, but we still need only do it once per lattice, and we already had to compute each $\#\operatorname{Aut}(L)$ in order to check the mass formula. This would not have helped us much because almost all but 686 of our lattices L have $\operatorname{Aut}(L) = \{\pm 1\} \times W_L$ (see (6.3) below), so lattices with the same R_L almost always have the same $\operatorname{Aut} L$ as well. But there may be similar problems where $[\operatorname{Aut} L : \pm W_L]$ provides more information.

- Finally we can include the lattice $M \supset L$. This need not run counter to our desire for an independent check of correctness, because we can recover M from L using the construction in Proposition 3, and then find it in Table 2 using $R(M)$. In our data, lattices with the same $\sigma(L)$ often have the same M as well; for instance the four batches with $\mu \geq 10$ all come from the last M in Table 2, with $R(M) = A_7^2 D_5$. But again in similar situations one or more gluing constructions could contribute to a useful signature.

6. Tables and features of the data

We collect here some statistics about the 167889 lattices L and their invariants.

6.1. **Counts of lattices L by Mordell–Weil torsion and rank.** We start by tabulating, for each $r = 1, \ldots, 11$ and each cyclic group T of order ≤ 4, the number of lattices whose Mordell–Weil rank $r_{\mathrm{MW}} = 18 - \operatorname{rk}(R(L))$ equals r and whose Mordell–Weil torsion $T_{\mathrm{MW}} = R^+(L)/R(L)$ is isomorphic with T. These are the only ranks and torsion groups that arise. Empty cells indicate a count of zero; for example, $|T| = 2$ implies Mordell–Weil rank at most 8. The final column and row count the totals of lattices with a given torsion group and rank respectively.

$T_{\mathrm{MW}} \backslash\ r_{\mathrm{MW}}$	1	2	3	4	5	6	7	8	9	10	11	Σ
$\{0\}$	11	397	3858	16964	38304	48316	36146	15778	4067	471	21	164333
$\mathbf{Z}/2\mathbf{Z}$	8	126	632	1175	989	385	57	2				3374
$\mathbf{Z}/3\mathbf{Z}$	2	21	76	47	13							159
$\mathbf{Z}/4\mathbf{Z}$	2	7	12	2								23
Σ	23	551	4578	18188	39306	48701	36203	15780	4067	471	21	167889

Table 5: Counts of lattices L by Mordell–Weil torsion $T_{\mathrm{MW}}(L) = R^+(L)/R(L)$ and $r_{\mathrm{MW}}(L) = 18 - r(R)$

6.2. **Counts of lattices L by glued lattice M, Mordell–Weil torsion, and Mordell–Weil rank.** We next count lattices according to the triple $(M, T_{\mathrm{MW}}, r_{\mathrm{MW}})$. Only 27 of the $16 \cdot 4 = 64$ possible pairs (M, T_{MW}) arise. Instead of attempting a three-dimensional table, we exhibit 27 rows, one for each pair (M, T_{MW}). The lattices M are listed in the order of Table 2, identified by their root lattices $R(M)$. For each M, most of its slices L have trivial T_{MW}; when some also have nontrivial torsion, we give first the row for trivial T_{MW}, then the other(s) marked with "+". The same convention applies to the final column, which gives the total L counts for each (M, T_{MW}) pair. Again empty cells indicate a count of zero. For example, there are 7871 lattices with trivial torsion obtained as slices of the rank-19 lattice M with $R(M) = A_1 D_{10} E_7$, and another 711 lattices with torsion $\mathbf{Z}/2\mathbf{Z}$; of those, only one has rank 1, and that one has nontrivial torsion. For $R(M) = D_6^3$, there are 13949 lattices with trivial torsion and 682 with torsion $\mathbf{Z}/2\mathbf{Z}$, with none of rank 1 and six of rank 2, each with torsion $\mathbf{Z}/2\mathbf{Z}$. The 21 lattices of maximal rank (namely rank 11), and the two lattices with nontrivial torsion and maximal rank (namely $|T_{\mathrm{MW}}| = 2$ and $r_{\mathrm{MW}} = 8$), are all slices of the lattice M with $R(M) = A_7^2 D_5$.

$R(M) \setminus r$	1	2	3	4	5	6	7	8	9	10	11	Σ
D_{19}	3	12	7									22
$D_{11}E_8$	2	36	104	70	7							219
$A_3E_8^2$	2	35	158	167	66	7						435
A_3D_{16}	1	40	132	203	81	7						464
+ $[\mathbf{Z}/2\mathbf{Z}]$	4	27	67	36	5							+139
D_7D_{12}	1	36	209	437	278	36						997
$D_5E_7^2$		20	194	583	663	299	40					1799
$A_{15}D_4$	1	22	180	611	996	738	161	6				2715
+ $[\mathbf{Z}/2\mathbf{Z}]$	1	15	46	83	47	13						+205
A_1A_{17}	1	32	298	990	1429	761	83					3594
+ $[\mathbf{Z}/3\mathbf{Z}]$	2	16	39	20	4							+81
E_6^3		7	154	755	1679	1816	952	187	9			5559
+ $[\mathbf{Z}/3\mathbf{Z}]$		3	9	7	1							+20
$A_3D_8^2$		10	169	1037	2240	2135	882	132	3			6608
+ $[\mathbf{Z}/2\mathbf{Z}]$		6	53	109	106	32	2					+308
$A_1D_{10}E_7$		35	517	2184	3182	1700	250	3				7871
+ $[\mathbf{Z}/2\mathbf{Z}]$	1	35	196	319	148	12						+711
D_6^3			53	634	2587	4667	3911	1761	324	12		13949
+ $[\mathbf{Z}/2\mathbf{Z}]$		6	46	182	274	150	24					+682
$A_1^2A_{11}E_6$		14	277	1708	4251	5308	3422	908	63			15951
+ $[\mathbf{Z}/3\mathbf{Z}]$		2	28	20	8							+58
A_9^2		18	273	1345	3918	6413	5739	2449	414	10		20579
$A_{11}D_7$		58	718	3570	8562	9808	5156	877	22			28771
+ $[\mathbf{Z}/2\mathbf{Z}]$	2	30	177	319	261	80	6					+875
+ $[\mathbf{Z}/4\mathbf{Z}]$	2	7	12	2								+23
$A_7^2D_5$		22	415	2670	8365	14621	15550	9455	3232	449	21	54800
+ $[\mathbf{Z}/2\mathbf{Z}]$		7	47	127	148	98	25	2				+454
Σ	23	551	4578	18188	39306	48701	36203	15780	4067	471	21	167889

Table 6: Counts of lattices L by M_L, torsion, and rank

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

6.3. **Quotients** $\mathrm{Aut}(L)/\pm W_L$**; minimal and maximal numbers of automorphisms.** Every lattice has a central involution -1. For our lattices L this involution cannot be contained in W_L, because W_L acts trivially on the quotient $L/R(L)$, and this quotient has positive rank (we do not need Table 5 for this: the discriminant of a root lattice of rank at most 18 must be a product of primes no larger than 19). Hence $\mathrm{Aut}(L)$ always has a normal subgroup $\pm W_L = \{\pm 1\} \times W_L$. For most of our 167889 lattices L, this subgroup $\pm W_L$ is the full automorphism group. The exceptions are 670 lattices with $[\mathrm{Aut}(L) : \pm W_L] = 2$, and 16 with $[\mathrm{Aut}(L) : \pm W_L] = 3$. Curiously each of the lattices L with $[\mathrm{Aut}(L) : \pm W_L] = 3$ has rank 3, 6, or 9; all of these have trivial Mordell–Weil torsion. The lattices L with $[\mathrm{Aut}(L) : \pm W_L] = 2$ include at least one lattice of rank r for each of the 11 ranks in Table 5; of these, 15 have Mordell–Weil torsion $\mathbf{Z}/3\mathbf{Z}$, and the remaining 655 have trivial torsion. Table 7 gives the counts for each case.

$[\mathrm{Aut}(L) : \pm W_L] = 2$:

(r,T)	$(1,1)$	$(1,2)$	$(2,1)$	$(2,2)$	$(3,1)$	$(3,2)$	$(4,1)$	$(4,2)$	$(5,1)$	$(5,2)$
#	1	2	7	1	55	8	75	2	184	2

$[\mathrm{Aut}(L) : \pm W_L] = 2$:

r	6	7	8	9	10	11
#	116	140	37	33	5	2

$[\mathrm{Aut}(L) : \pm W_L] = 3$:

r	3	6	9
#	3	9	4

Table 7: Counts of lattices L with $[\mathrm{Aut}(L) : \pm W_L] = 2$ or 3 by Mordell–Weil rank r and torsion size T ($T = 1$ if $[\mathrm{Aut}(L) : \pm W_L] = 2$ and $r \geq 6$; also $T = 1$ for all L with $[\mathrm{Aut}(L) : \pm W_L] = 3$)

The lattices with the minimal $\#\mathrm{Aut}(L)$, and thus the largest contribution to the total mass, are the five lattices L with $R(L) \cong A_1^5 A_2$ (which are among the 21 that attain the minimal rank of $R(L)$, and thus the maximal Mordell–Weil rank). Each of these has $\mathrm{Aut}(L) = \pm W_L \cong (\mathbf{Z}/2\mathbf{Z})^6 \times S_3$, a group of order $2^7\,3 = 384$. The next-smallest $\mathrm{Aut}(L)$ is $(\mathbf{Z}/2\mathbf{Z})^9$, of size 512, for the three lattices with $R(L) \cong A_1^8$. The smallest $\mathrm{Aut}(L)$ that properly contains $\pm W_L$ has order $2^7\,3^2 = 1152$ and appears for a unique L, one of the five with $R(L) \cong A_1^3 A_2^2$.

The largest automorphism groups are those of the lattices $L = L_0 \oplus \Lambda$ that arose in the previous section, where L_0 is the lattice with Gram matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 82 \end{smallmatrix}\right)$, and Λ is one of the two even lattices of rank 16 and discriminant 1. In each case $\mathrm{Aut}\, L = \mathrm{Aut}\, L_0 \times \mathrm{Aut}\, \Lambda$, and $\mathrm{Aut}\, L_0 = \pm W_{L_0} \cong (\mathbf{Z}/2\mathbf{Z})^2$. It has often been noted that of the two choices of Λ, the root lattice E_8^2 has the larger automorphism group $W_{E_8}^2 \rtimes S_2$ (so $L_0 \oplus E_8^2$ has the largest automorphism group of our 167889), though it's quite close, with ratio 405/286 (and $405 + 286$ supplying the Bernoulli factor 691 of the mass formula for even lattices of rank 16 and discriminant 1).

6.4. **Multiplicities of root lattices** $R(L)$ **and saturated root lattices** $R^+(L)$**.** There are 1402 different root lattices that appear as $R(L)$ for one of our 167889 lattices L, and 1504 that appear as $R^+(L)$. Thus in each case the average multiplicity must exceed 100. In fact both the most common $R(L)$ and the most common $R^+(L)$ is $A_1^2 A_2 A_3 A_4$, appearing 3650 times. Table 8 shows the five most common R and their multiplicities, which are the multiplicities exceeding 2000.

R	$A_1^2 A_2 A_3 A_4$	$A_1^3 A_2 A_3 A_4$	$A_1^2 A_2 A_3 A_5$	$A_1^3 A_2 A_3^2$	$A_1 A_2^2 A_3 A_4$
#	3650	2708	2484	2387	2298

Table 8: The five most common root lattices

On the low-multiplicity side, there are 93 root lattices R that arise as $R(L)$ only once, and 105 lattices that arise as $R^+(L)$ just once. Each of the possible Mordell–Weil ranks $18 - \operatorname{rk} R = r = 1, 2, \ldots, 11$ appears at least once among these R.

r	1	2	3	4	5	6	7	8	9	10	11
$\#R$	19	28	13	2	3	10	5	5	4	3	1
$\#R^+$	23	28	14	4	3	11	7	7	4	3	1

Table 9: Number of $R(L)$ or $R^+(L)$ of rank $18 - r$ that determine L uniquely

The only $r = 11$ case is $R(L) = R^+(L) = A_2^2 A_3$. There are also two root lattices, both with $r = 1$, that appear once as $R^+(L)$ and just once more as $R(L) \neq R^+(L)$, namely A_{17} (with $[R^+(L) : R(L)] = 1$ or 3) and $A_2 A_{15}$ (with $[R^+(L) : R(L)] = 1$ or 2).

7. Availability of the results

We hope that the lattices L and their invariants will eventually find a permanent home in the LMFDB [LMFDB 2026]. For now, they are publicly available online at the directory

`http://abel.math.harvard.edu/~elkies/L/18/163/`

which contains:

- A file GRAM.gp.bz2 (112.5M, compressed to 9.27M) containing a GP vector G of Gram matrices for the 167889 lattices L;
- A file SIG.gp.bz2 (10M, compressed to 1M) containing a GP vector SIG of the signatures for those lattices;
- A file M.gp containing a GP vector M of Gram matrices for the 16 lattices M,
- A file V.gp.bz2 (6.8M, compressed to 0.66M) containing a GP vector V of lists V[1], ..., V[16] of integer vectors of length 19 that encode the hyperplane slices giving the lattices in GRAM.gp.bz2, in the same order.

The signature vectors give the following information:

(1) The name of $R(L)$ (for example, `A1^2A2A3A4` for $A_1^2 A_2 A_3 A_4$, the most common root lattice);

(2) The Mordell–Weil rank $r_{\mathrm{MW}}(L) = 18 - \operatorname{rk} R(L)$;

(3) The structure of the Mordell–Weil torsion group $T_{\mathrm{MW}}(L) = R^+(L)/R(L)$;

(4) The discriminant of $R(L)$;

(5) The number of components of $R(L)$ (e.g. `5` for $A_1^2 A_2 A_3 A_4$), which is the number of reducible fibers of the associated elliptic fibration;

(6) The counts $\mathrm{N}_{2m}(L)$ for $m = 1, 2, 3$;

(7) The counts $\mathrm{N}_{2m}(R^+(L))$ for $m = 2, 3$;

(8) The size $\#\mathrm{Aut}(L)$ of the automorphism group of L; and

(9) The index $[\mathrm{Aut}(L) : W_{R(L)}]$.

Some of this information is redundant: $R(L)$ determines all of the Mordell–Weil rank, $\operatorname{disc} R(L)$, the count of components, and $\mathrm{N}_2(L)$; and $R(L)$ together with $\#\mathrm{Aut}(L)$ determines $[\mathrm{Aut}(L) : W_{R(L)}]$. We nevertheless include these statistics to simplify some searches. We still omit $\mathrm{N}_{2m}(R^+(L))$ for $m = 1$ because it is the same as $N_2(L)$ which already appears.

Acknowledgements. I thank the referees for their careful reading and detailed comments. This research was supported in part by the National Science Foundation, Grant DMS-1502161, and Simons AGNTC Collaboration, Grant #550031.

References

[Allombert–Chenevier 2025] Bill Allombert and Gaëtan Chenevier: Unimodular hunting II, *Forum of Mathematics, Sigma* **13** (2025) e136. arXiv: 2410.19569 ; https://hal.science/hal-04765491v1 ; DOI: https://doi.org/10.1017/fms.2025.10058 .

[Chenevier–Taïbi 2026] Gaëtan Chenevier and Olivier Taïbi: Unimodular lattices of rank 29 and related even genera of small determinant, arXiv:2601.19780 (https://arxiv.org/abs/2601.19780).

[Conway–Sloane 1982] John H. Conway and Neil J. A. Sloane: The unimodular lattices of dimension up to 23 and the Minkowski–Siegel mass constants, *European J. Combinatorics* **3** (1982), 219–231; ≅ [Conway–Sloane 1999, Chapter 16].

[Conway–Sloane 1999] John H. Conway and Neil J. A. Sloane: *Sphere Packings, Lattices and Groups* (3rd ed.), New York: Springer 1999.

[Elkies 2007] Noam D. Elkies: Three lectures on elliptic surfaces and curves of high rank. arXiv:0709.2908 .

[Elkies 2018] Noam D. Elkies: K3 surfaces and elliptic fibrations in number theory, presentation at workshop 18w5190 "Geometry and Physics of F-theory" (BIRS, Banff, Alberta, Canada), January 2018. See https://archytas2.birs.ca/workshops/2018/18w5190/files/Noam_D_Elkies.pdf page 24 (26 in the PDF). Talk video: https://archytas2.birs.ca/events/2018/5-day-workshops/18w5190/videos/watch/201801231402-Elkies.html .

[Elkies–Klagsbrun 2020] Noam D. Elkies and Zev Klagsbrun: New rank records for elliptic curves having rational torsion. In: *ANTS XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, https://msp.org/obs/2020/4-1/obs-v4-n1-p15-s.pdf ; arXiv: 2003.00077 .

[Fincke–Pohst 1985] U. Fincke and M. Pohst: Improved Methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis, *Math. of Computation* **44** #170 (April 1985), 463–471; https://www.jstor.org/stable/2007966 .

[LMFDB 2026] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, http://www.lmfdb.org, 2026.

[Nebe–Sloane 2026] Gabriele Nebe and Neil J. A. Sloane: A Catalogue of Lattices, https://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/ (accessed 24 January 2026).

[Nishiyama 1996] Ken-ichi Nishiyama: The Jacobian fibrations on some K3 surfaces and their Mordell–Weil groups, *Japan. J. Math.* **22** (1996), 293–347.

[OEIS 2026] *Online Encyclopedia of Integer Sequences*, Sequence A005134: Number of n-dimensional unimodular lattices (or quadratic forms). https://oeis.org/A005134 (accessed 24 January 2026).

[PARI 2025] The PARI Group, PARI/GP version 2.17.1, Univ. Bordeaux, 2025, http://pari.math.u-bordeaux.fr/ .

[PARI doc] The PARI Group, online documentation: Vectors, matrices, linear algebra and sets, https://pari.math.u-bordeaux.fr/dochtml/html/Vectors__matrices__linear_algebra_and_sets.html .

[Plesken–Souvignier 1997] W. Plesken and B. Souvignier: Computing Isometries of Lattices, *J. Symb. Comput.* **24** #3–4 (Sept. 1997), 327–334; SN 0747-7171, doi:10.1006/jsco.1996.0130 .

[Sage 2023] William A. Stein et al.: Sage Mathematics Software (Version 9.8), The Sage Development Team, 2023, http://www.sagemath.org .

[Schütt 2010] Matthias Schütt: K3 surfaces with Picard rank 20. *Algebra and Number Theory* **4**:3 (2010); `https://msp.org/ant/2010/4-3/ant-v4-n3-p04-s.pdf`, arXiv: 0804.1558 .

[Schütt–Shioda 2019] Matthias Schütt and Tetsuji Shioda: *Mordell–Weil Lattices.* Singapore: Springer, 2019 (*Ergebnisse der Math. und ihre Grenzgebiete, 3. Folge*, **70**).

[Serre 1973] Jean-Pierre Serre, *A Course in Arithmetic.* New York: Springer, 1973.

[Venkov 1978] B. B. Venkov, The classification of integral even unimodular 24-dimensional quadratic forms, *Proc. Steklov Inst. of Math.* (1980 #4), 63–74; published two years earlier in Russian (*Trudy Mat. Inst. imeni V. A. Steklova* **148** (1978), 65–76); ≅ [Conway–Sloane 1999, Chapter 18].

Noam D. Elkies
Mathematics Department
Harvard University
1 Oxford Street
Cambridge, MA 02138 USA
elkies@math.harvard.edu