The 167889 even lattices of rank 18 and discriminant 163

ANTS-XVII (Groningen, the Netherlands),

9 July 2026

Noam D. Elkies, Harvard University

Overview

1. What?

2. Why?

3. How?

Overview

1. What?

• What's the problem — i.e., what does "even lattices of rank 18 and discriminant 163" mean?

• What's the solution — i.e., how do we present and describe each of those lattices L?

2. Why?

Why do we (you and I) care about this $(18, 163)$ case?

3. How?

How did we find those L and check that they're all different?

Lattices: definitions

Lattice of rank $r = \mathrm{rk}(L)$: geometrically, a discrete copy L of $\mathbf{Z}^r$ in Euclidean space $\mathbf{R}^r$, up to $\mathrm{Aut}(\mathbf{R}^r) = \mathrm{O}_r(\mathbf{R})$ (not just $\mathrm{SO}_r(\mathbf{R})$).

Algebraically, a **positive-definite** quadratic form $Q : \mathbf{Z}^r \to \mathbf{R}$, associated to symm. bilinear form $\langle \cdot, \cdot \rangle : \mathbf{Z}^r \times \mathbf{Z}^r \to \mathbf{R}$ with $Q(x) = \langle x, x \rangle$. [In this talk, $(r_+, r_-) = (r, 0)$ only.]

In geometric picture, Q and $\langle \cdot, \cdot \rangle$ are the quadratic norm and dot product on $\mathbf{R}^r$. Equivalence: $\mathrm{Aut}(\mathbf{Z}^r) = \mathrm{GL}_r(\mathbf{Z})$, invertible $\mathbf{Z}$-linear changes of variable — NB $\det = \pm 1$, not just $\mathrm{SL}_r(\mathbf{Z})$.

Gram matrix: $G = (\langle e_i, e_j \rangle)_{i,j=1}^r$, so $\langle v, v' \rangle = v^\top G v'$ ($v, v' \in \mathbf{R}^r$, column vectors). Equivalence: $G \sim B^\top G B$ for $B \in \mathrm{GL}_r(\mathbf{Z})$.

The *discriminant* $\mathrm{disc}(L)$ is $\det(G)$, well-defined because $(\det B^\top)(\det B) = (\det B)^2 = 1$. Geometrically, $\mathrm{disc}\, L = \mathrm{Vol}(\mathbf{R}^r / L)^2$.

Lattices: rational, integral, even

We say lattice L is *rational* (*integral*) if $\langle v, v' \rangle \in \mathbf{Q}$ (respectively, $\langle v, v' \rangle \in \mathbf{Z}$) for all $v, v' \in L$; equivalently: if all entries of Gram matrix G are rational (resp. integral).

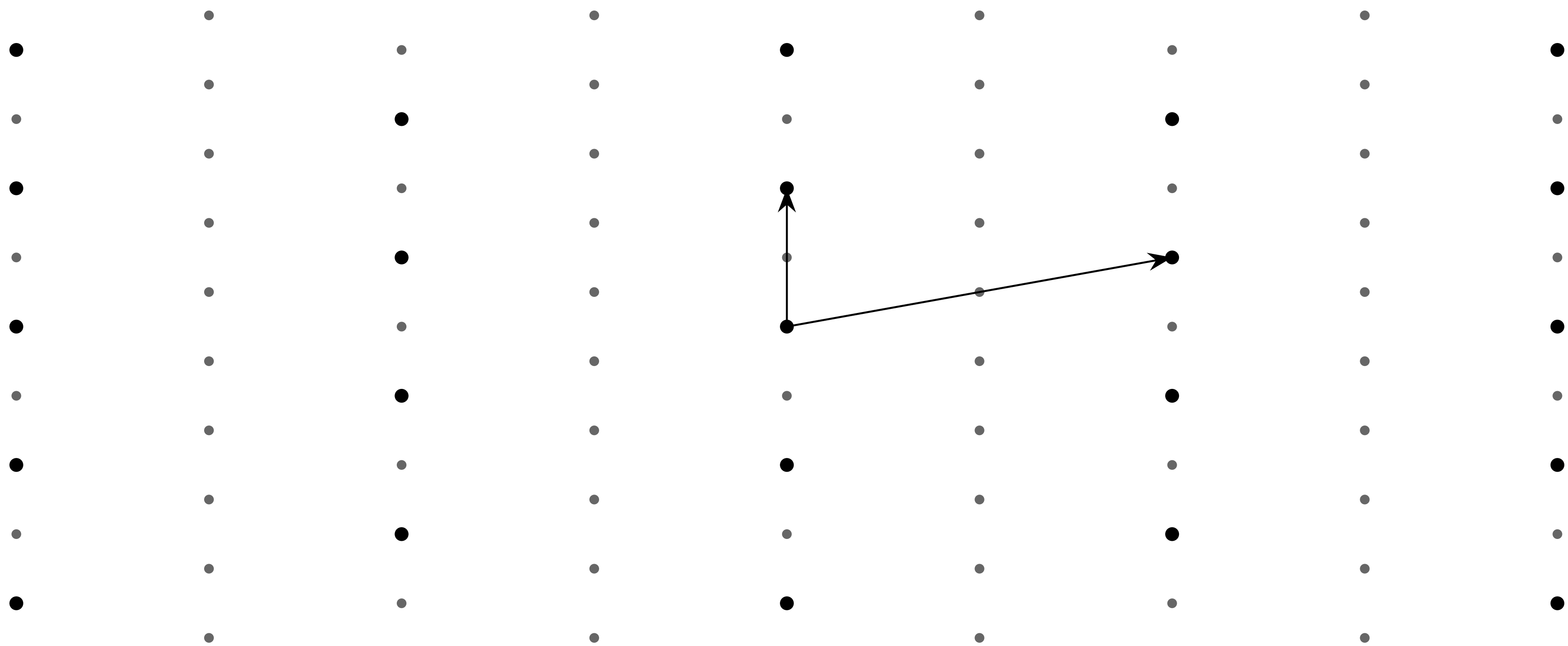
If L is integral, the identity

$$\langle v + v', v + v' \rangle = \langle v, v \rangle + \langle v', v' \rangle + 2\langle v, v' \rangle$$

gives a group homomorphism $h : L \to \mathbf{Z}/2\mathbf{Z}$, $v \mapsto \langle v, v \rangle \bmod 2$. We say L is *even* if $h = 0$, i.e. $\forall v \in L : \langle v, v \rangle \in 2\mathbf{Z}$; equivalently: G has all diagonal entries $\langle e_i, e_i \rangle$ even. Else L is *odd*, in which case it has an index-2 sublattice $\ker h = \{v \in L : \langle v, v \rangle \in 2\mathbf{Z}\}$ called the *even sublattice* of L.

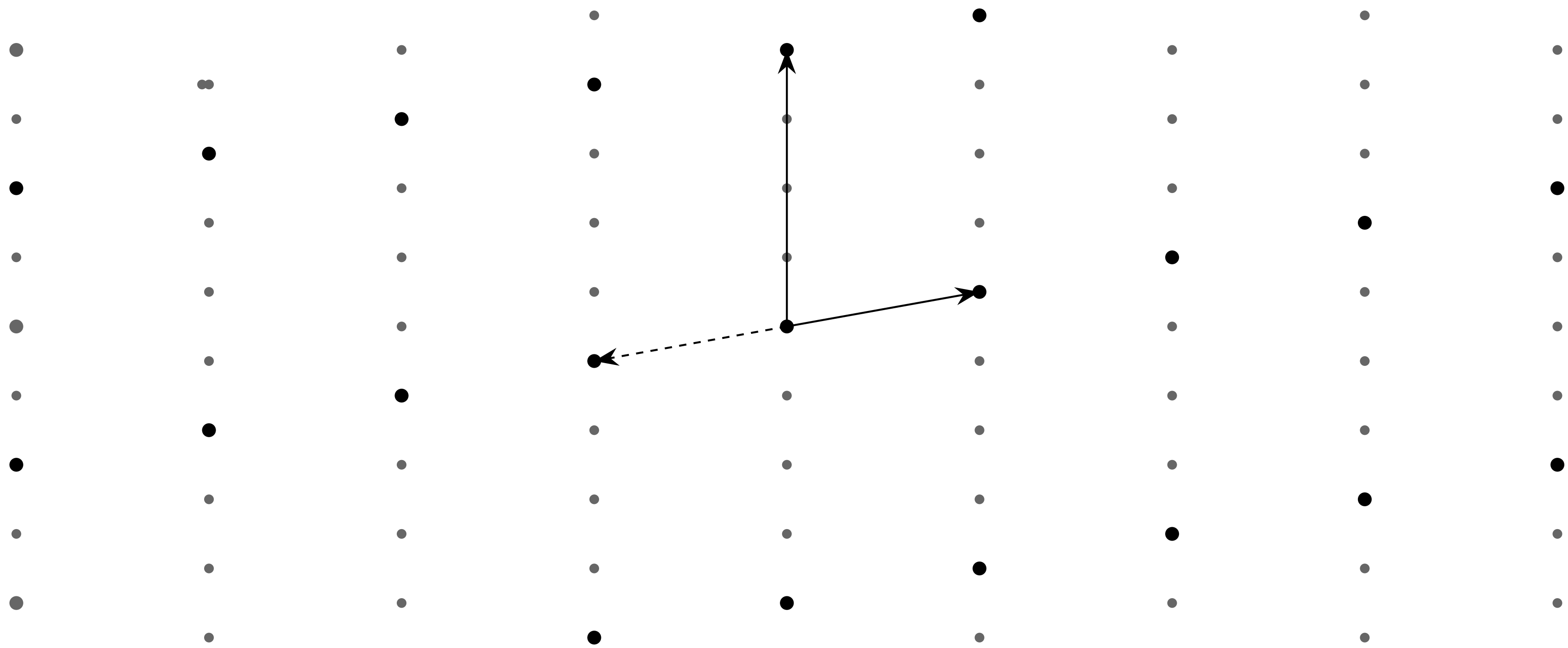
Given r and Δ there are finitely many isomorphism classes of integral rank-r lattices L with $\operatorname{disc} L = \Delta$. Depending on the choice of (r, Δ), these may include some even L.

Example: the two even lattices of rank 2 and discriminant 31



$$G = \begin{bmatrix} 16 & 1 \\ 1 & 2 \end{bmatrix}$$

Example: the two even lattices of rank 2 and discriminant 31



$$G = \begin{bmatrix} 4 & 1 \\ 1 & 8 \end{bmatrix} \sim \begin{bmatrix} 4 & -1 \\ -1 & 8 \end{bmatrix}$$

Problem, part 1 of 3

A fundamental result [Mordell?]: for $\Delta = 1$, there is an even lattice of rank r iff $r \equiv 0 \bmod 8$.

From this one eventually characterizes all (r, Δ) that arise for some even lattice. For example, if $r \equiv 2 \bmod 4$ then $\Delta \equiv 0$ or $3 \bmod 4$.

We can now start answering "What's the problem?":

Find all even lattices with $(r, \Delta) = (18, 163)$**.**

This we already did and briefly announced, in 2018.

A bit more about lattices: shells and roots

For the rest of the problem, we need some more lattice notions.

First we introduce shells and roots. $\mathbf{R}^r$ is loc. cpct., L discrete $\Rightarrow \#(L \cap \overline{B}_\mu(0)) < \infty$ for all μ. Thus for all m the shell

$$L_{(m)} := \{v \in L : \langle v, v \rangle = m\}$$

is finite (use $\mu = m^{1/2}$). Let $N_m(L) = \#L_{(m)}$. This is an invariant of L, with $N_0(L) = 1$ and $N_m(L) \equiv 0 \bmod 2$ for $m \neq 0$ by symmetry $v \leftrightarrow -v$. For L integral (resp. even), $N_m(L) = 0$ for all $m \notin \mathbf{Z}$ (resp. $m \notin 2\mathbf{Z}$).

Roots, continued

The possible shells $L_{(m)}$ can be described fully for $m = 1, 2$ (and probably not beyond), via projection and reflection maps

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

for nonzero $\alpha \in L$. If $\langle \alpha, \alpha \rangle = 1$ then π_α takes L to L, and we soon deduce: if $N_1(L) = 2k$ then $L = \mathbf{Z}^k \oplus L_1$ for a lattice $L_0 = L_{(1)}^{\perp} \cap L$ of rank $r - k$ with $N_1(L_0) = 0$.

$m = 2$: vectors $\alpha \in L$ with $\langle \alpha, \alpha \rangle = 2$ are called *roots* of L; their $\mathbf{Z}$-span is the *root lattice* $R(L)$. While π_α need not take L to L, the reflection s_α does act on L (and on $R(L)$), generating a normal subgroup $W_L = W_{R(L)}$ of $\mathrm{Aut}(L)$, the *Weyl group*.

Structure theorem: $R(L)$ is uniquely $\oplus_i R_i$, each R_i being one of A_n $(n \geq 1)$, D_n $(n \geq 4)$, or E_n $(n \in \{6, 7, 8\})$.

Problem, part 2 of 3

The *saturated root lattice* is $R_+(L) := (R(L) \otimes_{\mathbf{Z}} \mathbf{Q}) \cap L$. The quotient $R_+(L)/R(L)$ is a finite group, usually trivial but not always.

> **For the even lattices with $(r, \Delta) = (18, 163)$, compute invariants such as $N_2(L)$, $N_4(L)$, and the rank and structure of $R(L)$ and $R^+(L)$; and compile statistics for their distribution.**

Partly done in 2018; fortunately for $r = 18$ this is computationally routine. Much more information now (2026), and all of it is made public.

For example, Table 5 gives the counts of lattices L by their Mordell–Weil rank $r_{\mathrm{MW}}(L) = 18 - r(R(L))$ and Mordell–Weil torsion group $T_{\mathrm{MW}}(L) = R^{+}(L)/R(L)$:

$T_{\mathrm{MW}} \setminus r_{\mathrm{MW}}$	1	2	3	4	5	6
$\{0\}$	11	397	3858	16964	38304	48316
$\mathbf{Z}/2\mathbf{Z}$	8	126	632	1175	989	385
$\mathbf{Z}/3\mathbf{Z}$	2	21	76	47	13	
$\mathbf{Z}/4\mathbf{Z}$	2	7	12	2		
Σ	23	551	4578	18188	39306	48701

$T_{\mathrm{MW}} \setminus r_{\mathrm{MW}}$	7	8	9	10	11	Σ
$\{0\}$	36146	15778	4067	471	21	164333
$\mathbf{Z}/2\mathbf{Z}$	57	2				3374
$\mathbf{Z}/3\mathbf{Z}$						159
$\mathbf{Z}/4\mathbf{Z}$						23
Σ	36203	15780	4067	471	21	167889

The notations $r_{\mathrm{MW}}(L)$ and $T_{\mathrm{MW}}(L)$ come from elliptic fibrations of K3 surfaces, to be explained under "Why?".

Problem, part 3 of 3

So we wrote and ran some code and got oodles of output. But code can have errors. How do we know the output is correct? It's easy to check that each G in the output is the Gram matrix of an even lattice with $(r, \Delta) = (18, 163)$, but we need more:

> **Check independently that each isomorphism class of even** $(18, 163)$ **lattices is repreented exactly once in the output.**

That is, check (without rerunning the search code) that our list neither omits any lattices nor contains any isomorphic pair of lattices. This was done in 2026.

Why?

The study and classification of quadratic forms hardly requires justification: it has long been recognized as a central topic and tool in number theory, from Diophantine equations to number fields to automorphic forms, and figuring also in algebraic geometry and topology (e.g. pairings on H^* and H_*), group theory, cryptography, mathematical physics, and elsewhere.

One may still legitimately question the interest of our very special case of the even $(18, 163)$ lattices. I offer three reasons:

1) Many more lattices than previously* feasible to classify;
2) Techniques widely applicable to other parameter choices;
3) Connection w/elliptic fibrations of special K3 surface X_{163}.

1) Many more lattices than previously* feasible . . .

Conway–Sloane "SPLAG" = *Sphere Packings, Lattices and Groups* (1989, 1993, 1998–9), Ch.15 "On the Classification of Intgral Quadratic Forms" Introduction: for $r \geq 7$, "it seems that the forms are inherently unclassifiable" once $r + \Delta^{1/2}$ goes [much] beyond 24 due to combinatorial explosion.

E.g. $(r, 1)$ long stalled at $r = 25$ (Borcherds 2000, # = 665), though very recently $r = 28$ and even $r = 29$ was reached, in CPU-years (# = 374062, 38966352 [OEIS A054911], see Chenevier–Taïbi, arXiv:2601.19780 — invite them to speak at ANTS-18 !).

Our $r + \Delta^{1/2}$ is $18 + 163^{1/2} \sim 30.77$, in just a few CPU-hours. So, for $r \lesssim 18$ (relevant to K3 geometry), still much scope to go even further.

2) Techniques widely applicable to other (r, Δ)

We use the "gluing method" going back ~30 years to Witt–Kneser and Nishiyama. In our setting: $L \longleftrightarrow (\overline{M}, M, v^*)$ up to isomorphism, where

- $\overline{M}$ = one of the sixteen $(19, 1)$ lattices,
- M = even sublattice of $\overline{M}$ (so $(19, 4)$), and
- $v^* \in M^*$ [dual lattice, stay tuned] with $Q(v^*) = 163/4$.

Then $L = \{v \in M : \langle v^*, v\rangle = 0\}$ in $(v^*)^\perp$.

For much smaller "values of 163" this could be done by hand. But for $(18, 163)$ most M have so many v^*, even mod $\mathrm{Aut}(M) = \mathrm{Aut}(\overline{M})$, that we had to automate the search, and also the eventual correctness check.

This now applies to other $(18, p)$ for prime $p = 8k + 3$, and before long should be available for other (r, Δ).

3) Connection w/ell. fibrations of special K3 X_{163}

Very briefly (since in this context it's just extra motivation): some even lattice classifications with $r \lesssim 18 \longleftrightarrow$ models of a K3 surface X. Used in algebraic geometry to study K3's and their moduli, in math. physics, and in Dioph. record hunting.

Elliptic fibration: $\mathrm{NS}(X) \cong L\langle -1\rangle \oplus \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Shioda–Tate theorem: Mordell–Weil group of generic fiber $= L/R(L)$, so in particular its rank r_{MW} and torsion T_{MW} are $r - r(R(L))$ and $R^+(L)/R(L)$.

For Diophantine records, we need all of $\mathrm{NS}(X)$ defined over $\mathbf{Q}$. So $r = \rho - 2 \leq 18$, with $r = 18$ possible only when $\exists$ elliptic curve $E/\mathbf{Q}$ with CM of discriminant $-\Delta$ [Schütt], i.e.

$$\Delta \in \{3, 4, 7, 8, 11, 12, 16, 19, 27, 28, 43, 67, 163\}.$$

How?

Duality and gluing

About "$v^* \in M^*$" ...

For a lattice L in the Euclidean space $L_{\mathbf{R}} = L \otimes_{\mathbf{Z}} \mathbf{R}$, the *dual lattice* L^* is defined by

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

This is indeed a lattice in $L_{\mathbf{R}}$, and its dual L^{**} is L again. If $(e_i)_{i=1}^r$ is a basis for L with Gram matrix $G = (\langle e_i, e_j\rangle)_{i,j=1}^r$, then L^* has a dual basis with Gram matrix G^{-1}. In particular $\operatorname{disc} L^* = (\operatorname{disc} L)^{-1}$.

If L is rational then so is L^*. If L is integral, L^* need not be integral, but it does contain L, with $[L^* : L] = \operatorname{disc} L$.

We need L^* at several steps of the project.

If L is integral, $\langle\cdot,\cdot\rangle$ descends to perfect $(\mathbf{Q}/\mathbf{Z})$-valued pairing on the "discriminant group" $\Delta_L := L^*/L$. Subgroup $G \subset \Delta_L$ is isotropic for this pairing <ins>iff</ins> its preimage in L^* is still integral.

If L is even, this pairing has a refinement to a quadratic map $q_L : \Delta_L \to \mathbf{Q}/2\mathbf{Z}$. Now $G \subset \Delta_L$ is strongly isotropic <ins>iff</ins> its preimage in L^* is still (integral and) even.

Direct sums $L \oplus L'$ induce direct sums of duals, Δ_L, and q_L.

For $r \equiv 2 \bmod 8$, and **prime** $\Delta = p = 8k + 3$, the structure of q_L is uniquely determined. We use this to find strongly isotropic subgroup $G \subset \Delta_{L \oplus L'}$ of size p where $L' = (4p)$ of rank 1. The preimage of G in $L \oplus L'$ is our even lattice M, with

$$\text{disc}(M) = \frac{\text{disc}(L \oplus L')}{[(L \oplus L') : M]^2} = \frac{\text{disc}(L)\,\text{disc}(L')}{|G|^2} = \frac{(p)(4p)}{p^2} = 4.$$

This is "gluing" L to L', opposite of slicing M to recover L.

Choosing representatives v^* modulo Aut M

Knowing the 16 possible M, we must list for each one all $v^* \in M^*$ of norm $p/4$, up to action of $\mathrm{Aut}\, M$. But $\mathrm{Aut}\, M$ is huge, of order ranging from about $10^{13.1}$ to $10^{22.8}$ (the last is $2^{19}19!$, for $(\overline{M}, M) = (\mathbf{Z}^{19}, D_{19})$). Ouch!

Thankfully most of $\mathrm{Aut}\, M$ is the Weyl group W_M, and a Weyl group has the simplest possible fundamental cone, generated by e_i^* with each $\langle e_i^*, e_j^* \rangle \geq 0$. It's easy to loop over nonnegative combinations of the e_i^* up to norm $p/4$, and then check for minimality under the quotient group $\mathrm{Aut}(M)/W_M$, which for our M is always of size 2, 4, 8, or 12.

Verification

A necessary tool (at least to verify output): many instances of "Are L, L' isomorphic?". Will also need "What is $\#\,\mathrm{Aut}(L)$?".

gp routines **qfisom**, **qfauto** use [Plesken–Souvignier 1997]: reduce lattice isom/auto to graph isom/auto of enough shells to generate L (and L'). Problem: usually somewhat slow (need at least shell $L_{(4)}$, and $N_4(L) \sim 8000$ on average), and can be utterly infeasible — for $L = E_8^2 \oplus \begin{pmatrix} 2 & 1 \\ 1 & 82 \end{pmatrix}$ need $L_{(82)}$, of size 10^{14+}.

Solution: use L^* instead of L. Now we need fewer than 800 short vectors on average, and never as many as 10^5. Since $L \rightsquigarrow L^*$ is canonical, $\#(\mathrm{Aut}\,L) = \#(\mathrm{Aut}\,L^*)$, and $L \cong L'$ <u>iff</u> $L^* \cong L'^*$.

How to tell if the result is right?

The first few tries it won't be (bugs and math errors), so we need some easy sanity checks.

First, compare with previous work — not on $(18, 163)$ but $(18, p)$ for smaller $p \equiv 3 \bmod 8$. The smallest few p we found in the literature; others we'd already computed by mapping the 2-neighbor graph (more work but more output). Eventually those trial runs reproduced earlier results for $p \leq 67$ (and now also $p = 83$):

D	3	11	19	43	59	67
H	6	33	111	998	2751	4421

So the extension to $p \leq 163$ might be right too:

D	83	107	131	139	163
H	9657	26658	62916	82077	167889

Next check: Minkowski–Siegel mass formula.

Does the Minkowski mass of our list look right?

Using **qfisom** on each L^*:

$$\sum_L \frac{1}{\#(\mathrm{Aut}(L))} = \frac{419230817922826719935 87}{188813683430365593600 00} = \frac{47 \cdot 691 \cdot 1213 \cdot 3617 \cdot 294217150811}{2^{32}\, 3^{10}\, 5^4\, 7^2\, 11 \cdot 13 \cdot 17}$$

which is numerically 2.22034+. Prime factors 691 and 3617 include the numerators of Bernoulli numbers $B_{12} = -691/2730$ and $B_{16} = -3617/2730$ as they should.

Happily Sage agrees: the same number is the output of

(genera((18,0), 163, even=True)[0]).mass()

:-) Or, use the formula directly, computing the mass as

$$2^{-26}\prod_{k=1}^{8}|B_{2k}|\cdot\frac{163^{17/2}}{\pi^9}L(9,\chi_{163})$$

(exponent -26 is from $1-(3/2)18$), and

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

where $B_9 =$ Bernoulli polynomial $B_9(x) =$ "$[x+B]^9$", i.e.

$$\sum_{k=0}^{9}\binom{9}{k}B_{9-k}\,x^k = x^9 - \frac{9}{2}x^8 + 6x^7 - \frac{21}{5}x^5 + 2x^3 - \frac{3}{10}x.$$

Again the result matches our putative $\sum_L(1/\#\,\mathrm{Aut}(L))$.

We also need this value for the final step of our check.

Once the total mass of our list matches the formula, it's also easier to *prove* that our list is complete and free of duplicates, because proving either part establishes the other: extra lattices increase the mass; duplicates reduce it.

Problem: using the L^* trick, we're OK calling **qfauto** 167889 times; we are not happy running **qfisom** $\binom{167889}{2}$ times!

Solution: compute for each L some easy invariants (root configuration, shell count $N_4(L)$, etc.), collecting them into a signature $\sigma(L)$. Then we need only call **qfisom** on the pairs L, L' for which $\sigma(L) = \sigma(L')$. Bonus: $\sigma(L)$ includes $T_{\mathrm{MW}}(L)$ and $r_{\mathrm{MW}}(L)$.

This reduced the **qfisom** work factor from $\binom{167889}{2} \sim 1.4 \cdot 10^{10}$ to $14044 \sim 1.4 \cdot 10^4$.

Thankfully qfisom returned $\mathbf{0}$ each time, i.e. there is no such isomorphism, so the lattices are distinct as desired.

For further details, see the ANTS paper and the copious data online.

Thankfully qfisom returned $\mathbf{0}$ each time, i.e. there is no such isomorphism, so the lattices are distinct as desired.

For further details, see the ANTS paper and the copious data online.

Thankfully qfisom returned $\mathbf{0}$ each time, i.e. there is no such isomorphism, so the lattices are distinct as desired.

For further details, see the ANTS paper and the copious data online.

Thankfully qfisom returned **0** each time, i.e. there is no such isomorphism, so the lattices are distinct as desired.

For further details, see the ANTS paper and the copious data online.

Thankfully qfisom returned **0** each time, i.e. there is no such isomorphism, so the lattices are distinct as desired.

For further details, see the ANTS paper and the copious data online.

Thank you

THANK YOU