K3 surfaces and elliptic fibrations in number theory

Banff Workshop 18w5190:
Geometry and Physics of F-theory

23 January 2018

Noam D. Elkies, Harvard University

1. Examples of K3's and ell. fibrations in number theory

2. Shioda's "excellent families" of rational elliptic surfaces

3. An "excellent family" of K3 elliptic surfaces

4. A family of elliptically fibered CY3's of rank 10

1. Examples of K3's and elliptic fibrations in number theory

Overview:

Like elliptic curves (and more familiar building blocks such as rational functions, calculus, and Fourier analysis), K3 surfaces and elliptic fibrations are a central enough mathematical structure that "of course" they figure prominently also in some parts of number theory.

Number theorists need to know about varieties such as K3's, and invariants such as Néron-Severi groups, not just over $\mathbf{C}$ but also over small fields such as $\mathbf{Q}$ and even over finite fields such as $\mathbf{Z}/p\mathbf{Z}$.

1. Examples of K3's and elliptic fibrations in number theory

Overview:

Like elliptic curves (and more familiar building blocks such as rational functions, calculus, and Fourier analysis), K3 surfaces and elliptic fibrations are a central enough mathematical structure that "of course" they figure prominently also in some parts of number theory.

Number theorists need to know about varieties such as K3's, and invariants such as Néron-Severi groups, not just over $\mathbf{C}$ but also over small fields such as $\mathbf{Q}$ and even over finite fields such as $\mathbf{Z}/p\mathbf{Z}$.

WARNING: CONTAINS EXPLICIT MATERIAL

i) Diophantine equations

In general: rational solution of Diophantine equation $\Longleftrightarrow$ rational point on alg. variety V

Dim.1: rational, elliptic, or general type ($g \geq 2$).

Dim.2: K3's are analogous to elliptic curves; next level of difficulty past rational surfaces. (Not abelian surfaces? That's a closer analogue but much rarer in practice.)

Examples include simple equations, geom. constructions, algebraic identities, moduli spaces; these often overlap, and often give V with ρ at or near the maximum of 20 (thanks to symmetry or "trivial" divisors).

Euler already found parametric solutions (rational curves on V) for

$$(d^2, e^2, f^2) = (b^2 + c^2, c^2 + a^2, a^2 + b^2)$$

("Euler bricks", e.g. $(a, b, c; d, e, f) = (44, 117, 240; 267, 244, 125)$),

$$xyz(x + y + z) = a$$

(triangles with rational sides and given area $a^{1/2}$, for any $a \in \mathbf{Q}^*$), and

$$a^4 + b^4 = c^4 + d^4$$

(e.g. $(133, 134; 59, 158)$; NB in number theory that's very different from $a^4+b^4+c^4 = d^4$ and $a^4+b^4+c^4+d^4 = 0$!).

Also:

• Triangles with rational sides and medians: again 3 quadrics in $\mathbf{P}^5$, here $4m_c^2 = 2(a^2+b^2) - c^2$ etc.;

• Points at rational distances from the vertices of a unit equilateral triangle (the quartic surface

$$\sum_{i=0}^{3} x_i^4 = \sum_{0 \le i < j \le 3} x_i^2 x_j^2,$$

with distances x_i/x_0 for $i = 1, 2, 3$) $\Longleftrightarrow$ rational triangles with a rational Fermat distance;

• Pairs of Pythagorean triangles with the same area: $(ab(a^2-b^2) = cd(c^2-d^2)$, a quartic surface; here and later there are isolated ADE singularities to resolve before we get the smooth K3 model).

Examples from more "advanced" math:

• split sextics x^6+ax^2+bx+c (the roots satisfy $\sum_{i=1}^6 x_i^d = 0$ for $d = 1,2,3$, so a complete $(2,3)$ intersection in $\mathbf{P}^4$) [count mod p: 6th moment of exp. sums $\sum_{x=0}^{p-1} e^{2\pi i(rx^3+sx^2)/p}$];

• likewise, split quintics $x^5+ax^3+bx^2+c$ (the roots satisfy $\sum_{i=1}^5 x_i = \sum_{i=1}^5 1/x_i = 0$, so a quartic in $\mathbf{P}^3$) [count mod p: 5th moment of Kloosterman sums $\sum_{x=1}^{p-1} e^{2\pi i(rx+sx^{-1})/p}$];

• for $G = \mathbf{Z}/7\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}$, $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/6\mathbf{Z})$, and $(\mathbf{Z}/4\mathbf{Z})^2$, the universal elliptic curves over the modular curves $X_1(G)$, which parameterize elliptic curves with torsion G and a rational point;

• for any elliptic curve $E_0 : y^2 = x^3 + a_0x + b_0$: quadratic twists $cy^2 = x^3 + a_0x + b_0$ with two rational points (it's the Kummer of $E_0 \times E_0$).

ii) Moduli problems

Thanks to the Torelli theorem for K3 surfaces, there is a rich structure of moduli spaces, call them $\mathcal{K}_L$ for K3 surfaces, indexed by even lattices L of signature $(1, \rho-1)$ that embed primitively into the K3 lattice $U^3 \oplus E_8^2\langle -1\rangle$ (a.k.a. $\mathrm{II}_{3,19}$). Each $\mathcal{K}_L$ classifies K3's with isometric embedding $L \hookrightarrow \mathrm{NS}$; it is the union of components of dimension $20-\rho$, and embeds into $\mathcal{K}_{L'}$ for any primitive sublattice L'. [Here and earlier, "primitive": $L' = (L' \otimes \mathbf{Q}) \cap L$, so geometrically L' is a slice of L.]

These $\mathcal{K}_L$ are arithmetic quotients, and for large ρ include more familiar moduli varieties like modular curves (both classical and Shimura), the modular threefold $\mathcal{A}_2$ classifying principally polarized abelian surfaces (ppas), and the Humbert surfaces $\mathcal{M}_D \subset \mathcal{A}_2$ that classify ppas with real multiplication.

Remarkably some of these old moduli spaces are easier to get at via their $\mathcal{K}_L$ description than via the abelian surfaces that they parametrize. (One explanation is that the difficulty roughly groups with $|\mathrm{disc}\, L|$, and inclusions $\mathcal{K}_L \subset \mathcal{K}_{L'}$ let us deal even with moderately large $|\mathrm{disc}\, L|$, say $\lessapprox 10^3$, by organizing the calculation as a sequence of steps of difficulty measured by $|\mathrm{disc}\, L|\ /\ |\mathrm{disc}\, L'|$.)

This was done for some Shimura curves [NDE 2008]; and later, systematically, for Humbert surfaces $\mathcal{M}_D$, and with some further work also for the Hilbert surfaces "$Y_-(D)$" that cover $\mathcal{M}_D$ 2:1 and parametrize ppas with an action of $\mathcal{O}_D$. Not surprisingly, these $Y_-(D)$ tend to get more complicated as D increases, and a few are themselves K3; e.g. the first of these, $Y_-(21)$, is singular ($\rho = 20$) with discriminant $-1008 = 2^4 3^2 7$. [NDE-Kumar 2014] *iii) Diophantine records*

Record ranks for elliptic curves:

Theorem (Mordell c.1920): $E(\mathbf{Q})$ is finitely generated for any elliptic curve $E/\mathbf{Q}$.

Theorem (Mazur 1977): Torsion group $E(\mathbf{Q})_{\text{tors}}$ is either $\mathbf{Z}/N\mathbf{Z}$ for $1 \leq N \leq 10$ or $N = 12$ or $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2N\mathbf{Z})$ for $N = 1, 2, 3, 4$. (Each arises infinitely often: all 15 modular curves are rational.)

Open question: Given $E(\mathbf{Q})_{\text{tors}}$, what ranks are possible? Is the rank unbounded?

While it's open: can we find specific $E/\mathbf{Q}$ of high rank?

Standard strategy: start from a family of elliptic curves E_t with the target torsion group and moderately large rank; these are retained by most specializations (e.g. by Silverman for $t \in \mathbf{P}^1$), and then we search for t that have new points.

Simplest case is when the base of t's is $\mathbf{P}^1$, and then we have an elliptic surface. Rational elliptic surfaces have rank at most 8 (more on this later), so the next step is elliptic K3's.

Example: trivial torsion. General theory: $\rho \leq 20$ so MW rank ≤ 18. Can be attained over $\mathbf{C}$ (and thus over some number fields), e.g. $y^2 = x^3 + P_{12}(t)$ with icosahedral P_{12} [G.Zaytman found the MW lattice explicitly here]; but not over $\mathbf{Q}$! Why not? . . .

By Tate-Shioda (stated later), rank 18 implies that NS is $U \oplus L\langle -1\rangle$ with L of minimal norm 4. But if NS $=$ NS$_{\mathbf{Q}}$ then $D = |\mathrm{disc}\, L|$ is one of the 13 "Euler-Heegner numbers"

$$D = 3, 4, 7, 8, 11, 12, 16, 19, 27, 28, 43, 67, 163$$

for which the quadratic order of discriminant $-D$ has unique factorization [Schütt 2010]. And even 163 is too small — indeed it turns out that this surface has many thousands of elliptic fibrations but all of rank at most 11.

Fortunately, with much effort we found a single elliptic K3 surface of MW rank 17, from a sporadic rational point on a Shimura curve parametrizing a certain family of K3's with $(\rho, \mathrm{disc}) = (19, 948)$. This eventually produced $E_t/\mathbf{Q}$ of rank as large as 28 ([NDE 2006], and still the only known source of rank > 24). These curves also give new records for 2-rank of class group of cubic number fields [Klagsbrun-Sherman-Weigandt 2016].

Here's a simpler example where we *can* use the $(20, -163)$ surface. The general elliptic curve with 4-torsion is

$$y^2 + axy + aby = x^3 + bx^2$$

(torsion generator $(x, y) = (0, 0)$. Taking

$$(a, b) = ((8t - 1)(32t + 7),\ (t + 1)(15t - 8)(31t - 7))$$

yields $\mathrm{K3}/\mathbf{P}^1_t$ with Mordell–Weil group $(\mathbf{Z}/4\mathbf{Z}) \oplus \mathbf{Z}^4$; one choice of generators has x-coordinates

$$-\tfrac{15}{4}(t + 1)(31t - 7)(32t + 7),\ (8t - 1)(15t - 8)(31t - 7)(32t + 7),$$
$$-(t + 1)(8t - 1)(15t - 8)(32t + 7),\ -4(t + 1)(2t + 5)(15t - 8)(32t + 7).$$

$E_t/\mathbf{Q}$ for $t = 18745/6321$ has rank 12 (NDE 2006), the current rank record for torsion $\mathbf{Z}/4\mathbf{Z}$ (and all other known curves with MW group $(\mathbf{Z}/4\mathbf{Z}) \oplus \mathbf{Z}^{12}$ are of the form E_t too).

Curves of fixed genus $g > 1$:

Theorem (Faltings 1983, conjectured by Mordell c.1920): *Let C be an algebraic curve of genus $g > 1$ over a number field K. Then $|C(K)| < \infty$.*

Now fix K and $g > 1$, and vary C. Can that $|C(K)| < \infty$ get arbitrarily large? In other words: Is

$$B(g, K) := \sup_{C} |C(K)|$$

infinite?

Theorem (Caporaso-Harris-Mazur 1997): *Assume Bombieri-Lang conjecture. Then $B(g, K) < \infty$ for all $g > 1$ and K.*

The Bombieri-Lang conjecture is an analogue of Mordell-Faltings for algebraic varieties of arbitrary dimension:

Conjecture (Bombieri-Lang 1986): *Suppose V is an algebraic variety of general type. Then all its rational points are in a finite union of subvarieties V_i' each of dimension $< \dim(V)$.*

So, under Bombieri-Lang, we have $B(g, K) < \infty$ by C-H-M.

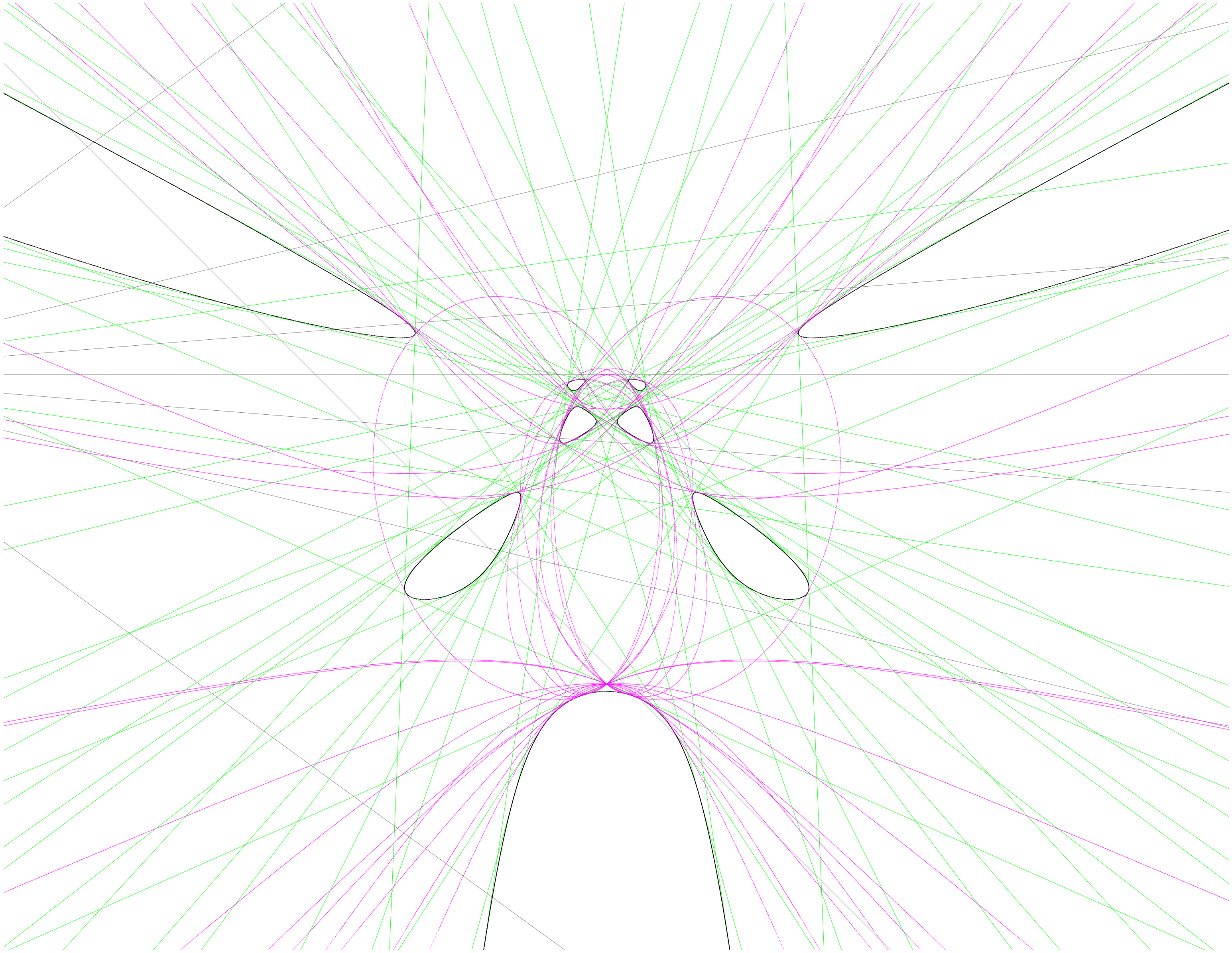
What's the Caporaso-Harris-Mazur bound on $B(g, K)$?

Alas the proof gives no explicit upper bound, because (as with Faltings) the argument is ineffective — as it must be: already for $\dim(V) = 1$ the exceptional V_i' are the rational points of the curve V, and in general we have no control over their number.

So again we're record hunting . . .

Genus 2: use a K3 surface with a degree 2 polarization, a.k.a. "double plane" $y^2 = P_6(x_0, x_1, x_2)$. Lines tangent to the sextic $P_6 = 0$ at three points lift to pairs of rational curves. Generic line $\ell \in \mathbf{P}^2$ lifts to a genus-2 curve with at least as many pairs of rational points as we have tritangent lines.

Here's such a model of the $(20, -163)$ surface:



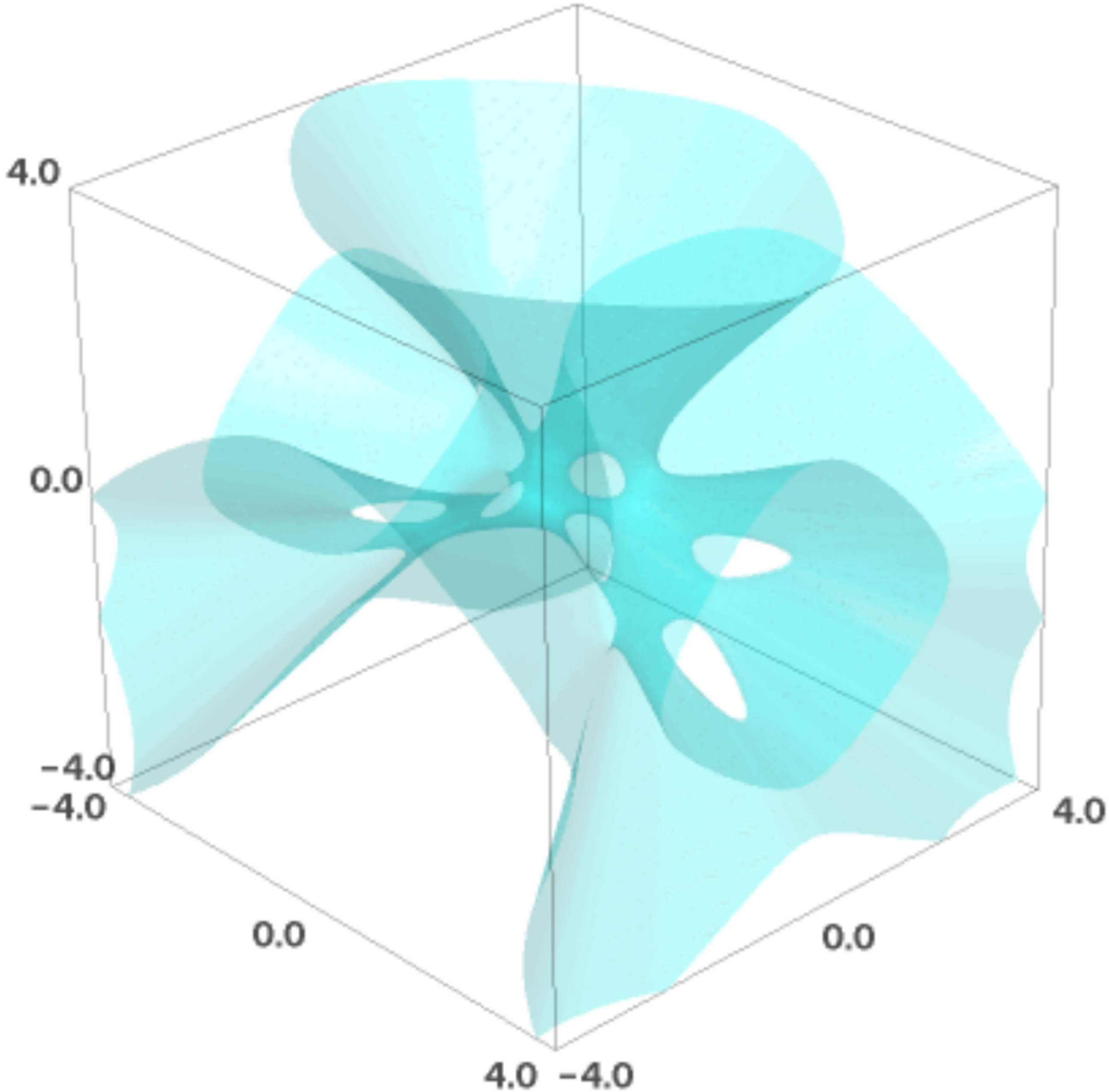
Current record (NDE + M.Stoll 2008–09): at least $2 \cdot 321$ points on

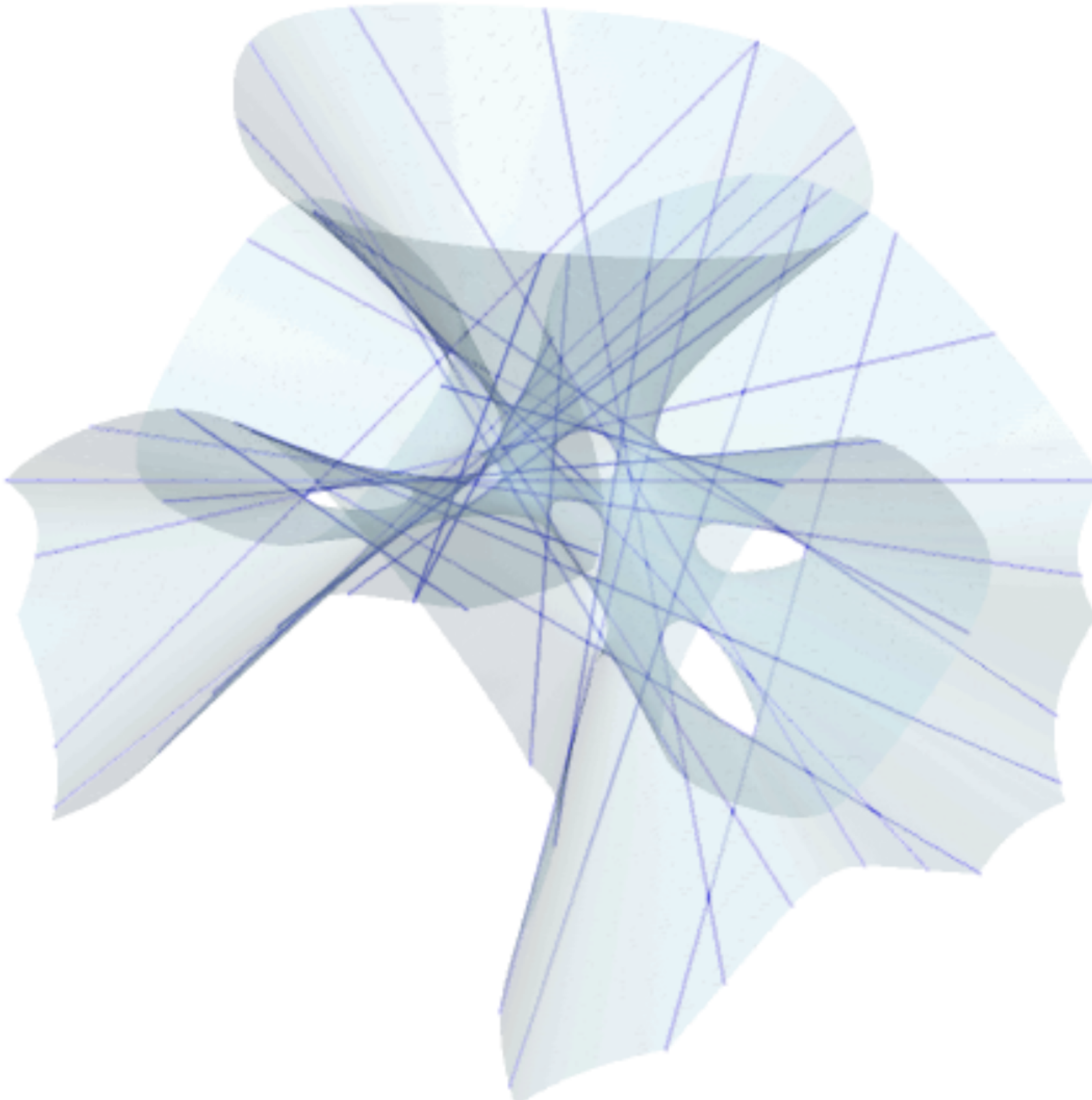
$$Y^2 = 82342800X^6 - 470135160X^5 + 52485681X^4 + 2396040466X^3 + 567207969X^2 - 985905640X + 15740^2,$$

with X equal

0, −1, −4, 4, 5, 6, 1/3, −5/3, −3/5, 7/4, . . . , 148596731/35675865, 58018579/158830656, 208346440/37486601, −1455780835/761431834, −3898675687/2462651894.

Likewise for genus 3 we try plane sections of a quartic K3 surface with many lines. Over $\mathbf{Q}$, the same $(\rho, \Delta) = (20, -163)$ surface has a smooth model with 46 lines; here's a nice picture of another model with 42:


4.0
0.0
-4.0
-4.0
0.0
4.0
-4.0
0.0
4.0



2. Elliptic fibrations

Genus-1 fibrations, and especially elliptic fibrations, are a useful tool for many of these problems. This is clear when hunting for elliptic-curve records; but such fibrations are prominent also in our other contexts.

• We can build on the rich structure and theory of elliptic curves. Euler already used this to find rational curves of "Euler bricks" and $a^4+b^4=c^4+d^4$ solutions by (as we now describe it) using the group structure to make new non-trivial solutions from trivial ones. Likewise we first found nontrivial rational solutions of $a^4+b^4+c^4=d^4$ using a genus-1 fibration.

• For an elliptic fibration of a surface S, the Tate-Shioda theorem relates the "arithmetic" of the fibration (reducible fibers, torsion and Mordell–Weil rank, canonical height of sections) with the geometry of the surface (intersection pairing on $\mathrm{NS}(S) = U \oplus L\langle -1 \rangle$: the MW group is L/R where R is the ADE lattice coming from reducible fibers).

• K3 surfaces can have numerous elliptic fibrations, corresponding to different decompositions $\mathrm{NS}(S) = U \oplus L'\langle -1 \rangle$ with L' "in the same genus" as L but not isomorphic. We've seen examples already; e.g.

$$y^2 = x^3 + Ax + (B_+ t + B + B_- t^{-1})$$

has elliptic fibrations x and t with $L = E_8 \oplus E_8$ and D_{16}^+ respectively. These are the only two fibrations for generic $A, B, B_\pm$, but our $(-20, 163)$ surface has a total of 167889 elliptic fibrations — each with $\mathbf{Q}$ coefficients for all equations and sections — corresponding to the 167889 even Euclidean lattices of rank 18 and discriminant 163. [This enumeration finished NDE 22.i.2018, just in time; MW ranks $1, \ldots, 11$. These lattices (= quadratic forms) and their genera are themselves of number-theoretic interest.]

Moreover, we can move systematically among them using "neighbor method" (L, L' are "p-neighbors" if they have isomorphic sublattices of index p; in practice we use $p = 2$ and maybe $p = 3$.) See e.g. [NDE-Kumar 2014], where we use this to move from a convenient elliptic fibration to one with E_7 and E_8 fibers (Kodaira II^*, III^*) and can apply Kumar's formulas for the Igusa-Clebsch invariants of the associated genus-2 curve. This let us and others search the rational points of these surfaces to find points whose corresponding ppas account for some Galois representations computed by other means.

3. Shioda's "excellent families" (1990+)

Suppose $S \to \mathbf{P}^1$ is a rational elliptic surface (DP8?) with an <u>additive</u> singular fiber (Type II, cusp) at $t = \infty$. Then the fibration has Weierstrass model

$$y^2 = x^3 + \left(\sum_{i=0}^{3} p_i t^i\right) x + \left(\sum_{j=0}^{5} q_j t^j\right).$$

Not unique because of affine maps $t \to \alpha t + \beta$ of $\mathbf{P}^1$ and scaling $(x, y) \to (\lambda^2 x, \lambda^3 y)$. Using these we may assume $\boxed{q_5 = 1 \text{ and } q_4 = 0}$. This leaves only multiplicative scalings, with total weight 30; thus p_i and q_j have weight $20-3i$ and $30 - j$ respectively:

t	x	y	p_3	p_2	p_1	p_0	q_3	q_2	q_1	q_0
6	10	15	2	8	14	20	12	18	24	30

The set of p_i and q_j weights should look familiar!

Shioda relates this with the Mordell–Weil lattice E_8 of

$$y^2 = x^3 + \left(\sum_{i=0}^{3} p_i t^i\right) x + \left(t^5 + \sum_{j=0}^{3} q_j t^j\right),$$

generated by 240 "roots" = sections (x, y) of the form

$$x = x_2 t^2 + x_1 t + x_0, \quad y = y_3 t^3 + y_2 t^2 + y_1 t + y_0$$

with $x_2^3 = y_3^2$, i.e. $(x_2, y_3) = (a^{-2}, a^{-3})$ with a of weight 1:

t	x	y	a	p_3	p_2	p_1	p_0	q_3	q_2	q_1	q_0
6	10	15	1	2	8	14	20	12	18	24	30

This a identifies the additive $t = \infty$ fiber with $\mathbf{G}_a$ (lemma: 3 points (a_i^{-2}, a_i^{-3}) on $Y^2 = X^3$ collinear $\iff \sum_{i=1}^{3} a_i = 0$).

The p_i and q_j determine the 240 a's up to the action of the Weyl group $W(E_8)$ — and what's "excellent" here and in a series of similar examples is that the coefficients p_i, q_j generate the invariant ring!

This is nice for number theory because it gives a family of rank-8 surfaces parametrized by $\mathbf{P}(\mathrm{Hom}(E_8, \mathbf{G}_a)) = \mathbf{P}^7$, a family of Galois extensions of generic Galois groups $W(E_8)$ (parametrized by t, p_i, q_j in appropriately weighted $\mathbf{P}^8$, etc.).

We also get a family of elliptic fibrations CY5 $\to \mathbf{P}^4$ by restricting to any linear $\mathbf{P}^4 \subset \mathbf{P}^7$ and specializing t to any sextic form on this $\mathbf{P}^4$.

Likewise for some of the other "excellent families" found by Shioda and others (Shioda-Usui, NDE, . . .). For example, Shioda's E_7 family, obtained by requiring the additive $t = \infty$ fiber to be not II (cusp) but III (two tangent $\mathbf{P}^1$'s):

$$y^2 = x^3 + (t^3 + p_1 t + p_0)x + \sum_{j=0}^{4} q_j t^j,$$

with 126 roots $(x,y) = (a^{-2}t^2 + O(t),\, a^{-3}t^3 + O(t^2))$ as before, and here also 56 dual roots with $(x,y) = (x_1 t + x_0,$ $at^2 + y_1 t + y_0)$; the weights are

t	x	y	a	p_1	p_0	q_4	q_3	q_2	q_1	q_0
4	6	9	1	8	12	2	6	10	14	18

so we get rank-7 elliptic fibrations CY3 $\to \mathbf{P}^2$ by restricting to a linear $\mathbf{P}^2 \subset \mathbf{P}^6$ and specializing t to any quartic form on this $\mathbf{P}^4$. As with the E_8 family, the coefficients for the 56 minimal sections are given by explicit polynomials.

But I'm told that rank-8 fibrations of CY3's are already known, so we must try harder to get a new record . . .

Some “excellent families” of K3 surfaces

Consider elliptic K3's $S \to \mathbf{P}^1$ of the special form

$$y^2 = x^3 + (p_7 t^7 + p_4 t^4 + p_1 t)x + (q_{12} t^{12} + q_9 t^9 + q_6 t^6 + q_3 t^9 + q_0)$$

with action of a symplectic 3-cycle $w : (t, x, y) \mapsto (\omega t, \omega^2 x, y)$ [“symplectic”: fixes the holomorphic 2-form $dt \wedge dx/y$].

The quotient is rational, with $(h^{2,0}, h^{1,1}, h^{0,2}) = (1, 8, 1)$; the ω and ω^2 eigenspaces each have just $h^{1,1}$, namely $(h^{2,0}, h^{1,1}, h^{0,2}) = (0, 6, 0)$, so contribute to NS($S$); it turns out that this rank-12 contribution is always the Coxeter-Todd lattice K_{12}, with $(\Delta, N_{\text{min}}, \kappa) = (3^6, 4, 756)$. NB the dimension of this family is right: $\rho = 2 + 12 = 14$, and $8 - 2 = 6 = 20 - \rho$.

Now we can set $q_{12} = 0$ so the fiber above the fixed point $t = \infty$ is a cusp, and normalize $p_7 = 1$ to get

$$y^2 = x^3 + (t^7 + p_4 t^4 + p_1 t)x + \left(\sum_{j=0}^{3} q_{3j} t^{3j} \right)$$

which is an "excellent family" associated to Mitchell's complex reflection group of K_{12} (defined over $\mathbf{Z}[\omega]$, Shephard-Todd #34):

t	x	y	p_4	p_1	p_9	q_6	q_3	q_0
4	14	21	12	24	6	18	30	42

But, while this is interesting for other reasons, it doesn't seem to give a rank-12 CY fibration over any $\mathbf{P}^{n-1}$, because the overall weight of 42 is just too large.

However, . . .

Setting also $p_7 = 0$ makes the $t = \infty$ fiber reducible of Type IV (three coincident lines), contributing A_2 to NS(S) and leaving a rank-10 Mordell–Weil lattice (called K_{10}^*):

$$y^2 = x^3 + (p_4 t^4 + p_1 t)x + \left(t^9 + \sum_{j=0}^{2} q_{3j} t^{3j}\right)$$

This is an "excellent family" for a reflection group in $U_5(\mathbf{C})$, Shephard-Todd #33:

t	x	y	p_4	p_1	q_6	q_3	q_0
2	6	9	4	10	6	12	18

Both the K_{12} and K_{10} families are NDE c.1999, used a few times since for tasks such as high-rank "Mordell curves" $y^2 = x^3 + a_6$. More recently W.Taylor mentioned the physics interest in high-rank fibrations of CY's, so:

4. A family of elliptically fibered CY3's of rank 10

Since p_4, p_1, q_6, q_3, q_0 are homogeneous forms of degrees $4, 10, 6, 12, 18$ on $\mathbf{P}^4$, we can restrict to a generic $\mathbf{P}^2 \subset \mathbf{P}^4$, and take for t any quadratic form on that $\mathbf{P}^2$, to get an elliptic fibration over $\mathbf{P}^2$ given by the same formula

$$y^2 = x^3 + (p_4 t^4 + p_1 t)x + \left(t^9 + \sum_{j=0}^{2} q_{3j} t^{3j}\right)$$

whose total space is birational CY3 for generic choices of the $\mathbf{P}^2$ and t. Moreover, the special choice $t = 0$ yields such fibrations of the special form $y^2 = x^3 + a_6$ with $a_6 \in \Gamma(O(18))$, obtained from a special degree-18 invariant of the ST33 reflection group, again by restriction to some $\mathbf{P}^2 \subset \mathbf{P}^4$.

THE END

Any (more) questions?