REAL MULTIPLICATION ABELIAN SURFACES OVER $\mathbb{Q}$

NOAM ELKIES

Recall:

New eigen-cuspforms f of weight 2 on $\Gamma_0(N)$ with $\mathbb{Q}(f)$ totally real and $[\mathbb{Q}(f) : \mathbb{Q}] = d$ $\longleftrightarrow$ dimension d factors of $J_0(N)$ $\longleftrightarrow$ abelian varieties $A/\mathbb{Q}$ of dimension d with real multiplication (=RM) by an order in $K = \mathbb{Q}(f)$ up to isogeny.

$d = 1$: elliptic curves, which we understand quite well: moduli (the j-line, $\cong \mathbb{P}^1$), explicit formulas (Weierstrass etc.), isogenies, etc.

$d > 1$: we understand these much less well.

I'll report on recent progress on the case $d = 2$. Already here we didn't even know what the general RM abelian variety looks like, even principally polarized with RM by the full ring of integers O_K, except for the simplest K (discriminant $D = 5$, 8, maybe 12?). That is, we know the moduli of the general ppas (principally polarized abelian surface), or almost equivalently of the Jacobian of the general curve of genus 2 — the moduli space $\mathcal{A}_2$ is 3-dimensional, rational, and birationally parametrized by the Clebsch(-Igusa) invariants; but except in the simplest cases we do not know equations in $\mathcal{A}_2$ for the moduli surfaces of ppas with RM.

We might expect that Cremona's extensive table of modular forms f would give us some idea what kind of RM surfaces we expect to find over $\mathbb{Q}$. See the next page for a table summarizing data on about 10^4 forms up to $N = 5000$ and a bit beyond. This collection of data is not entirely satisfactory in various ways[1], but it should still give a reasonable sense of "what's out there". We see that the smallest D's dominate the statistics as expected, but many larger D occur as well.

We also include for each $D = \mathrm{disc}(K)$ the type R, $K3$, E, or G (rational, K3, "honestly elliptic", or general) of the moduli surface $Y_-(D)$ of ppas with RM by O_K, as determined c.1975 by Hirzebruch–van de Ven (for prime D) and Hirzebruch–Zagier (for composite D). [We have no guarantee that a typical $d = 2$ factor of $J_0(N)$ has a principal polarization, but probably the moduli spaces for RM surfaces without such a polarization tend to be more complicated and thus to have sparser rational points; likewise for RM surfaces whose endomorphism ring has index > 1 in O_K.]

Date: September 28, 2007.

[1]It is extracted from a database created by William Stein and downloadable from http://modular.fas.harvard.edu/tables/arith_of_factors, titled "Arithmetic data about every weight 2 newform on $\Gamma_0(N)$ for all $N < 5135$ (and many more up to 7248)". While the sample of N is somewhat peculiar, I doubt that it produces a systematic bias among the $d = 2$ forms. Only the first ten a_p are tabulated; in all but a handful of cases $a_p \notin \mathbb{Z}$ for at least one of these p, so we can find K, which is sufficient for our table though sometimes it does not determine the RM *ring* in K. Also, one form may represent more than one isomorphism class of ppas (due to isogenies), and thus more than one point on the moduli surface; and several forms may represent ppas with the same moduli (due to twists) — for instance, for each of the four $D \geq 113$ for which forms with $\mathrm{disc}(K) = D$ are tabulated, there are two such forms but they are each other's twist.

D	Y_-	#	D	Y_-	#	D	Y_-	#	D	Y_-	#	D	Y_-	#
5	R	3552	33	$K3$	278	61	E	12	92	G	0	124	G	0
8	R	2490	37	$K3$	34	65	E	9	93	G	0	129	G	0
12	R	1410	40	$K3$	95	69	G	3	97	G	7	133	G	0
13	R	779	41	$K3$	110	73	G	37	101	G	0	⋯		
17	R	1080	44	E	21	76	G	11	104	G	0	145	G	2
21	R	221	53	E	0	77	G	0	105	G	0	⋯		
24	$K3$	329	56	G	6	85	G	3	109	G	6	184	G	2
28	$K3$	225	57	E	48	88	G	5	113	G	2	⋯		
29	$K3$	40	60	G	13	89	G	1	120	G	0	201	G	2

Both the R/K3/E/G classification and the observed modular forms suggest that it should be possible to go a lot further parametrizing and finding RM surfaces than the few $Y_-(D)$ parametrizations already in the literature. But how to do it?

The table also suggests that the R/K3/E/G data don't account for everything, e.g. $D = 29$ is underrepresented among the six K3 cases, and $D = 53$, alone among the honestly elliptic ones, is not seen at all. I can't explain this completely yet, but I do have various new explicit parametrizations and examples, including the first cases of $D = 53$, such as the Jacobians of

$$Y^2 = 2332X^6 + 902X^5 + 5060X^4 + 17111X^3 + 5995X^2 + 17545X + 27951$$

(the sextic has discriminant $2^{10}3^{12}11^{12}13^4 17^{10}$) and

$$Y^2 = 140450X^5 + 168540X^4 + 55703X^3 - 6572X^2 + 8706X + 5584$$

(yes, a quintic; disc. $= 2^8 3^{24} 5^8 13^8 53^6$). More examples and explanations later.

To start with, a bit more detail on the $\mathcal{A}_2$ moduli: a ppas A is uniquely the Jacobian $J(C)$ of some genus-2 curve C (or it's the product of two elliptic curves, but that's of positive codimension in $\mathcal{A}_2$, and won't show up in the tables of modular forms). Moduli for C: Clebsch(-Igusa) invariants $(I_2 : I_4 : I_6 : I_{10})$. So the surface $Y_-(D)$ will just be the vanishing locus of some weighted-homogeneous polynomial in those invariants… But that's the wrong way to go; these polynomials are ugly even in the simplest cases and will quickly get horrible even while the moduli space is still rational. Cautionary example from the familiar world of modular curves: $X_0(2)$ is rational, with coordinate $h = 2^{-6}(\eta(\tau)/\eta(2\tau))^{24}$ parametrizing 2-isogenies

$$y^2 = x^3 + ax^2 + bx \;\longleftrightarrow\; Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X$$

(with $a^2/b = 4(h+1)/h$) between elliptic curves of j-invariants $j = j(h) = 64(t+4)^2/t^2$ and $j' = j(1/h) = 64(4t+1)^3/t$; but if we insist on using (j, j') to exhibit $X_0(2)$ as a curve in $X_0(1) \times X_0(1)$ then it's a singular $(3,3)$ curve with some huge coefficients:

$$j^3 + j'^3 - (jj')^2 + 1488jj'(j+j') - 162000(j^2 + j'^2) \\ + 40773375jj' + 8748000000(j+j') - 157464000000000 = 0$$

and of course such formulas for $X_0(N)$ quickly get even worse. The same thing will happen for our moduli surfaces $Y_-(D)$. Moral: first find the moduli space on its own terms, then compute Clebsch(-Igusa) coordinates for the map $Y_-(D) \to \mathcal{A}_2$.

For all but the smallest D, imposing the RM condition directly on C or $A = J(C)$ gives a horrible mess. We go via the Kummer surface, birationally isomorphic with $A/\{\pm 1\}$:

$$C \longleftrightarrow J(C) = A \longleftrightarrow A/\{\pm 1\} \overset{\sim}{\longleftrightarrow} \mathrm{Km}(A)$$

It is known that $\mathrm{Km}(A) = \mathrm{Km}(J(C))$ is a K3 surface; moreover, For a generic genus-2 curve C, this K3 surface has Néron–Severi (NS) rank $\rho = 17$. But if A has RM, with endomorphisms by a real quadratic ring of discriminant D, then we get a further NS generator, raising the rank to 18, with discriminant $-16D$.[2] This brings us close to a region of the mathematical universe that I've been exploring for the past year or two, motivated initially by the problem of finding elliptic curves of large rank over $\mathbb{Q}(t)$ and $\mathbb{Q}$; besides attaining that goal, the exploration also opened up some other fruitful routes...

We would like to parametrize K3 surfaces S together with a primitive embedding into $\mathrm{NS}(S)$ of an even lattice L of signature $(1, 17)$ and reasonably small discriminant. The Kummer surfaces $\mathrm{Km}(A)$ do not quite fit the bill, both because the embedding $L \hookrightarrow \mathrm{NS}(S)$ is not usually defined over the ground field (it requires a choice of 2-torsion structure on A) and because of the large factor of 16 in $|\mathrm{disc}\, L|$. Fortunately we can do better by using not $\mathrm{Km}(A)$ but a related K3 surface S_A, constructed by Dolgachev[3]:

$$C \longleftrightarrow J(C) = A \longleftrightarrow A/\{\pm 1\} \overset{\sim}{\longleftrightarrow} \mathrm{Km}(A) \overset{2}{\longleftrightarrow} S_A.$$

That is, the K3 surfaces $\mathrm{Km}(A)$, S_A are related by degree-2 maps ("2-isogenies" — in fact the maps can be realized as 2-isogenies between elliptic surfaces). Thus they have the same Néron–Severi rank over an algebraic closure; but the Galois structures and discriminants of $\mathrm{Km}(A)$ and S_A may differ. Indeed here it turns out that in $\mathrm{NS}(S)$ we get a lattice of signature $(1, 17)$ consisting entirely of divisors defined over the ground field, and with discriminant $-D$ instead of $-16D$. The construction of S_A does not assume that A has RM; for a generic ppas A we get $\mathrm{NS}(S_A)$ of signature $(1, 16)$ and discriminant 2.

So, how to parametrize such a K3 surface? $\rho = 17$ or $\rho = 18$ makes a lot of conditions to impose on (say) a space quartic...

We find S as an *elliptic K3 surface*, that is, S together with an elliptic (a.k.a. Jacobian) fibration: a map $t : S \to \mathbb{P}^1$ such that the preimage of a generic point is an elliptic curve. [NB by definition an elliptic curve comes with an origin, i.e. our fibration must have a zero-section.] Then the surface is $y^2 = x^3 + \alpha(t)x + \beta(t)$ with α, β polynomials of degree at most $8, 12$ respectively.

Review of the basics of elliptic surfaces over $\mathbb{P}^1$, in particular elliptic K3 surfaces. In K3 case: the fiber and zero-section generate an even unimodular sublattice of signature $(1, -1)$ in $\mathrm{NS}(S)$, often called U, or H for "hyperbolic plane"; so $\mathrm{NS}(S) = U \oplus L_E\langle -1 \rangle$, where L_E,

---

[2] In general, the Torelli theorem for K3 surfaces (Piatetski-Shapiro and Šafarevič, 1971) gives, for each hyperbolic [i.e. of signature $(1, \rho - 1)$] even lattice L primitively contained in the K3 lattice $\mathrm{II}_{3,19}$ a nonempty moduli space of K3 surfaces S with primitive embeddings of L into $\mathrm{NS}(S)$, such that each component of the moduli space has dimension $20 - \mathrm{rk}(L)$. Here that's $20 - 17 = 3$ for generic C, and $20 - 18 = 2$ in each RM case, as it should be.

[3] Appendix to a paper by Galluzzi and Lombardo in the *Michigan Math. J.*, Vol. **52** (2004).

the "essential lattice" of the elliptic surface, is even, of rank $\rho - 2$, and positive definite (note the "$\langle -1 \rangle$"); for any such lattice the roots (vectors of norm 2) generate a sublattice R that is a direct sum of A_n's, D_n's, and E_n's, and here these factors correspond to the reducible fibers of the fibration (Kodaira symbol, computable by Tate's algorithm); and the Mordell–Weil group is canonically identified with L_E/R, with the induced quadratic form on $(L_E/R) \otimes \mathbb{Q}$ coinciding with the canonical height.

For the $\rho = 17$ surfaces corresponding to Jacobians of generic genus-2 curves, we want the even lattice L_E to have rank 15 and discriminant 2. There are two choices: either $L_E = R = E_7 \oplus E_8$, or $R = A_1 \oplus D_{14}$ and $[L_E : R] = 2$. We choose the former, and put the E_7 and E_8 fibers at $t = 0$ and $t = \infty$ respectively. By Tate's algorithm this means

$$\alpha(t) = at^4 + a't^3, \qquad \beta(t) = b''t^7 + bt^6 + b't^5$$

for some scalars a, a', b, b', b'' with a, b' nonzero. (Even though $\#\{a, a', b, b', b''\} = 5$, the moduli space has dimension $5 - 2 = 3$ as expected, because for any nonzero scalars λ, μ the scaling $(x, y, t) \leftarrow (\lambda^2 x, \lambda^3 y, \mu t)$ yields an isomorphic surface.)

So, this surface is $S_{J(C)}$ for some genus-2 curve C. What is C, and given C what are the coefficients of $S_{J(C)}$?

Theorem (A.Kumar, Ph.D. thesis 2006): *The Clebsch(-Igusa) invariants of C satisfy*

$$(\kappa^{-2} I_2, \kappa^{-4} I_4, \kappa^{-6} I_6, \kappa^{-10} I_{10}) = \left(-24\frac{b'}{a'},\ -12a,\ 96a\frac{b'}{a'} - 36b,\ 4a'b'' \right)$$

for some nonzero scalar κ. Equivalently, if the genus-2 curve C has invariants I_2, I_4, I_6, I_{10} then $S_{J(C)}$ can be taken to have coefficients

$$(a, a', b, b', b'') = \left(-\frac{I_4}{I_2},\ -1,\ \frac{I_2 I_4 - 3I_6}{108},\ \frac{I_2}{24},\ \frac{I_{10}}{2} \right).$$

Now $J(C)$ has RM by the quadratic order of discriminant D if and only if our elliptic surface $y^2 = x^3 + \alpha(t)x + \beta(t)$ has a section[4] of canonical height $D/2$. Simplest example: if $D = 5$, a section of canonical height $D/2$ is a solution $(x(t), y(t))$ of $y^2 = x^3 + \alpha(t)x + \beta(t)$ with x, y polynomials of degree 4, 6 respectively such that $t^2 | x$ and $t^3 | y$. [Geometrically this means a section of the elliptic fibration $t : S_{J(C)} \to \mathbb{P}^1$ that does not intersect the zero-section and passes through the non-identity simple component of the E_7 fiber at $t = 0$. Then the

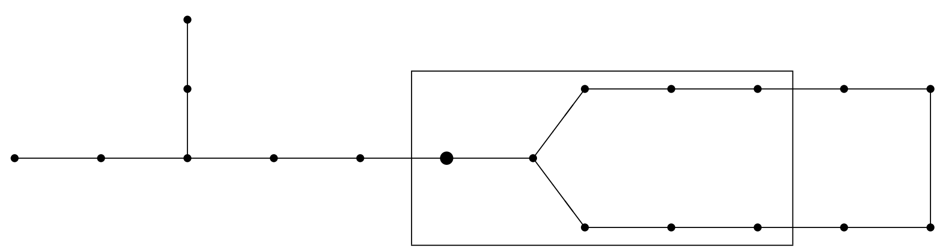
[4]In general, we may start with an admissible hyperbolic lattice $U \oplus L_E$ of rank ρ, choose a component of the moduli space of elliptic K3 surfaces with essential lattice containing L_E, and consider the codimension-1 subspaces on which the Néron–Severi rank is at least $\rho + 1$. These correspond to admissible lattices $U \oplus L'_E$ with L'_E a positive-definite even lattice that contains L_E with $L_E = (L_E \otimes \mathbb{Q}) \cap L'_E$. Let R' be the root lattice of L'_E. Necessarily $R' \supseteq R$ with $R = (R \otimes \mathbb{Q}) \cap R'$. Usually $R' = R$, and then our hypersurface is obtained by requiring that our elliptic surface have an extra section. But it is also possible for R' to strictly contain R. Geometrically this can happen in various ways: most simply, two I_1 fibers may merge to form an I_2 (in which case $L'_E = L_E \oplus A_1$ — we shall need this possibility later); but also a reducible fiber might become more singular by merging with an I_1, and it is even possible for two or more reducible fibers to merge. But when $L_E = R = E_7 \oplus E_8$, the only possibilities for R' other than R itself are $A_1 \oplus E_7 \oplus E_8$ and $E_8 \oplus E_8$. These yield $D = 4$ and $D = 1$ respectively. Then A is either $(2, 2)$-isogenous or isomorphic to a product of elliptic curves. These possibilities, and ones for which $D = D_0^2$ with $D_0 \geq 3$, are also interesting to parametrize (for instance, for $D_0 > 1$ we get Jacobians of curves of genus 2 with maps of degree D_0 to two elliptic curves), but are not usually regarded as examples of real multiplication.

section has naïve height 4 and canonical height $4-(3/2)=5/2$.] This is easy: choose x with square leading coefficient (three parameters); this determines y and a; then we choose a' (fourth parameter) and recover b, b', b''. So we're done, with a rational moduli space of the expected dimension of 2 — as before we subtract 2 from the number of parameters to account for scaling. Sanity check: do the resulting I_2, I_4, I_6, I_{10} from Kumar's formulas agree with the known parametrizations of genus-2 curves with this RM? Happily, yes.

Now try $D=33$ or $D=53$...Now we need to parametrize $x(t), y(t), \alpha(t), \beta(t)$ with α, β as above but $x=t^2\xi(t)/\delta(t)^2$ with ξ, δ polynomials of degrees 16, 7 respectively (for $D=33$) or 26, 12 (for $D=53$). What a mess!!

But this brings us back to our earlier warning: as with $X_0(2)$, we should first parametrize these K3 surfaces on their own terms, and only then find coordinates x, y, t that put them in the form $y^2=x^3+\alpha(t)x+\beta(t)$ that exhibits a copy of $U\oplus E_7\oplus E_8$ in the Néron–Severi lattice. To that end, we'll use elliptic fibrations in which L_E is generated by vectors of small norm.[5] For example, when $D=33$ a convenient choice is $L_E=R=A_{10}\oplus E_6$. We put the E_6 fiber at $t=0$ and the A_{10} at $t=\infty$. That is, $y^2=x^3+\alpha(t)x+\beta(t)$ where this time the E_6 fiber means $t^3|\alpha$ and $t^4\|\beta$, and the A_{10} fibers means that $\Delta := 4\alpha^3+27\beta^2$, normally a polynomial of degree 24, should have an zero of order 11 at $t=\infty$ when considered as a section of $O(24)$ on $\mathbb{P}^2$, so $\deg\Delta = 24-11=13$. The parametrization of such α, β, though still not quite trivial, is entirely feasible.

Having done it, we want to recover the $U\oplus E_7\oplus E_8$ form of the resulting K3 surfaces S. That is, we must find a copy of $U\oplus E_7\oplus E_8$ in $\mathrm{NS}(S)=U\oplus A_{10}\oplus E_6$, and construct a new elliptic fibration of S from the sections of an isotropic generator of the factor U of that $U\oplus E_7\oplus E_8$. This can be done, but the linear algebra (over a function field in two variables!) is unpleasant. It is better to proceed in stages. For example, the $A_{10}\oplus E_6$ form gives us the following diagram of (-2) curves generating $\mathrm{NS}(S)$:



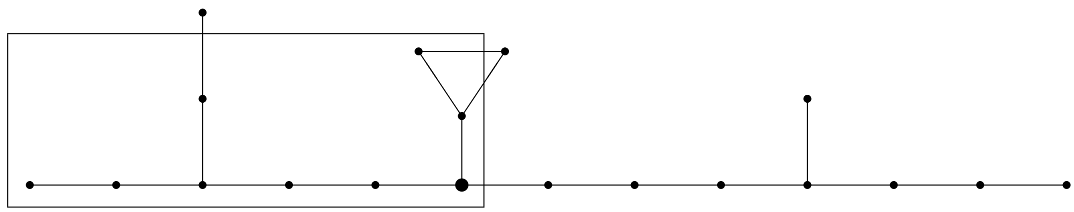
Two circles are joined if and only if the corresponding (-2) curves meet; the large circle represents the zero-section of the fibration, the cycle of 11 circles to its right are the components of the A_{10} fiber, and the 7 circles to the left are the components of the E_6 fiber. The box encloses an extended Dynkin diagram for the E_7 root system. Thus we can form a positive linear combination D of the eight (-2) curves represented by the vertices of the diagram such that $D^2=0$ and D is an E_7 fiber of a new elliptic fibration[6] on S. The sections of D

[5]It might be an even better heuristic to use a lattice basis $(v_1, v_2, \ldots, v_{16})$ that is small in the LLL "norm" $\sup_{i=1}^{16}\mathrm{disc}(\langle v_1,\ldots,v_i\rangle)/\mathrm{disc}(\langle v_1,\ldots,v_{i-1}\rangle)$.

[6]In general such a construction might yield a genus-1 fibration without a section; but here there is at least one divisor D' such that $D\cdot D'=1$, so we can use D' as the section. Specifically, either of the rightmost vertices in the box represents a component of D of multiplicity 1, so we may use for D' the (-2) curve represented by its neighbor outside the box.

form a two-dimensional space, and the quotient of any two generators yields a map $S \to \mathbb{P}^1$ that realizes the new elliptic fibration.

This fibration has an E_7 fiber as desired, but not an E_8 as well. To get at its other reducible fiber, note that any of our (-2) curves not in or adjacent to the E_7 box is orthogonal to D, and thus a component of some reducible fiber. This gives copies of A_2 and E_6 in the root lattice, and it turns out that our new fibration has $R = A_2 \oplus E_6 \oplus E_7$, with Mordell–Weil group isomorphic to $\mathbb{Z}$ and generated by a section of height $\mathrm{disc}(L_E)/\mathrm{disc}(R) = 33/(3\cdot3\cdot2) = 11/6$. Ignoring that section for now, we obtain the following diagram of (-2) curves:



The box encloses an extended E_8 root system, and proceeding as before we finally obtain our desired $U \oplus E_7 \oplus E_8$ form of S.

...except that we're not quite done. We can detect the remaining obstacle by using Kumar's formulas to recover I_2, I_4, I_6, I_{10}, then calculating (by Mestre's formulas, implemented in `Magma`) a genus-2 curve C with these invariants. We then compute, for various primes p of good reduction, the characteristic polynomial of the Frobenius map φ on C mod p. If $J(C)$ has real multiplication by $\mathbb{Z}[(1+\sqrt{33})/2]$, then $\varphi + p\varphi^{-1}$ satisfies a quadratic equation whose discriminant is 33 times a square. This happens, but only half the time; for the other p's, we find that $(\varphi + p\varphi^{-1})^2 \in \mathbb{Z}$. The reason is that $J(C)$ indeed has an endomorphism e with $e^2 + e = 8$, but e is defined not over $\mathbb{Q}$ but over a quadratic extension F, so e and $1-e$ are indistinguishable, and remain so mod p if p is inert in F. The same difficulty occurs for any D, not just $D = 33$. On the level of moduli spaces, the problem is that the map from $Y_-(D)$ to $\mathcal{A}_2$ is not birational to its image but a $2:1$ cover. The image is birational with $Y_-(D)/\{1,\iota\}$, where ι is the following involution: a generic point on $Y_-(D)$ gives an ordered pair (A, e) where A is a ppas and e is an endomorphism $(D+\sqrt{D})/2$ of A;[7] the involution ι takes (A, e) to (A, e') where e' is the endomorphism $(D-\sqrt{D})/2$. Thus a generic point on $Y_-(D)/\{1,\iota\}$ gives a ppas with not a distinguished endomorphism $(D+\sqrt{D})/2$ but a conjugate pair of such endomorphisms.

To get at $Y_-(D)$ itself, we thus need a double cover of the moduli surface of K3 surfaces that we have constructed. The branch locus is where e is equivalent to $1-e$ [in general: where the endomorphism $(D+\sqrt{D})/2$ of $J(C)$ is equivalent to $(D-\sqrt{D})/2$] under conjugation in $\mathrm{End}(J(C))$. This makes $\mathrm{End}(A)$ an order in a quaternion ring, adding a 19th generator to the Néron–Severi groups of $\mathrm{Km}(J(C))$ and $S = S_{J(C)}$. In our $D = 33$ setting, this means that $\mathrm{NS}(S)$ has discriminant 66, not -33, coming from an extra reducible fiber of type A_1 in the $A_{10} \oplus E_6$ fibration. Equivalently, $\Delta = 4\alpha^3 + 27\beta^2$ has a double root other than $t = 0$ (and $t = \infty$). So the desired branch locus is obtained by setting the discriminant of the cubic Δ/t^8 equal to zero. Along the way we've also parametrized a previously inaccessible

[7] Actually it might not be right to say that "a generic point on $Y_-(D)$ (or on $Y_-(D)/\{1,\iota\}$) gives a ppas" at all: in general there is an obstruction in $\mathrm{Br}(K)[2]$ to finding a ppas over K corresponding to a given K-rational point on $\mathcal{A}_2$. But this difficulty is separate from the problem of recovering $Y_-(D)$ from its image in $\mathcal{A}_2$.

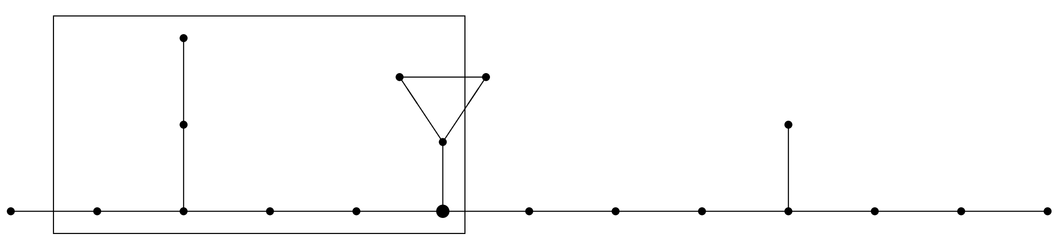
Shimura curve in $Y_-(33)$. [For general D, the surface S must have $\operatorname{disc}(\mathrm{NS}(S)) = 2D$, unless $8|D$ when both $2D$ or $D/2$ are possible. The systematic use of K3 surfaces of rank 19 to parametrize and study Shimura curves is a separate topic, and will be treated at length elsewhere.]

Once we have the branch locus, we know $Y_-(D)$ over $\mathbb{C}$, at least if $Y_-(D)/\{1, \iota\}$ is simply connected (which it certainly is in all cases computed so far, including $D = 33$ and $D = 53$, because then $Y_-(D)/\{1, \iota\}$ is actually rational); at any rate we have it up to finitely many choices. Over $\mathbb{Q}$, we also have to find the correct quadratic twist. But there are finitely many choices there too, because $Y_-(D)$ must have good reduction at all primes not contained in D. We pinpoint the correct twist by starting from any point on $Y_-(D)/\{1, \iota\}$ not in the branch locus and reducing mod p for a few small primes p of good reduction. This finally gives us the desired equations for $Y_-(D)$ as well as ι and the map $Y_-(D) \to \mathcal{A}_2$.

In the $D = 33$ example, we birationally identify $Y_-(33)/\{1, \iota\}$ with $\mathbb{P}^2$, and $Y_-(33)$ with the double cover obtained by extracting the square root of the sextic given (in affine coordinates) by

$$9s^6 - (26r^2 - 80r + 104)s^4 + (25r^4 - 152r^3 + 400r^2 - 408r + 432)s^2 - (2r-2)^3(r^3 - 6r^2 + 14r + 2)$$

This not only confirms that $Y_-(33)$ is a K3 surface but also lets us obtain more precise information about it; for instance, we find enough divisors to prove that $Y_-(33)$ is a "singular K3 surface", that is, a K3 surface whose Néron–Severi rank over $\bar{\mathbb{Q}}$ attains its maximum of 20 in characteristic zero, and also to identify the lattice $\mathrm{NS}(Y_-(33))$ — in particular, $\operatorname{disc}\mathrm{NS}_{\bar{\mathbb{Q}}}(Y_-(33)) = -99$. The formula also shows that $Y_-(33)$ has another involution, commuting with ι, that lifts the involution of $\mathbb{P}^2$ given in affine coordinates by $(r, s) \longleftrightarrow (r, -s)$. This involution takes a ppas A with real multiplication by $\mathbb{Z}[(1 + \sqrt{33})/2]$ to an isogenous abelian surface $A' = A/G$ where G is the kernel of multiplication by an ideal of norm 3 in $\mathbb{Z}[(1 + \sqrt{33})/2]$; the fact that the square of this ideal is principal yields a principal polarization on A'. In our diagram of (-2) curves for $R = A_2 \oplus E_6 \oplus E_7$, we reach A' instead of A by changing the boxed E_8 diagram to this one:



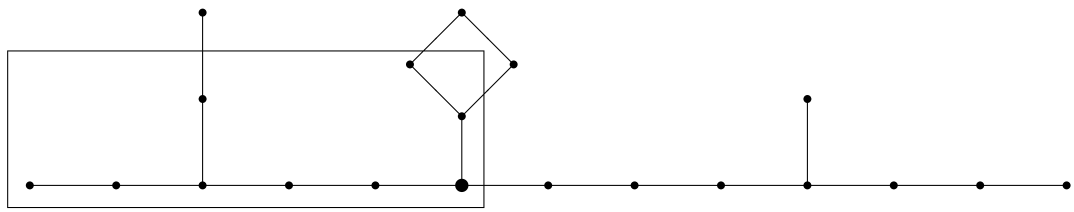
Here's an explicit example of a pair of genus-2 curves related by this isogeny: if $(r, s) = (1, \pm 3)$ then our sextic equals 72^2, so we have rational points on $Y_-(33)$; the corresponding curves are

$$Y^2 = -(X^3 - 3X - 1)(4X^3 - 3X + 5), \qquad Y^2 = -(X^3 - 3X + 1)(8X^3 - 9X^2 - 6X - 1).$$

The fact that each right-hand side factors as a product of cubics reflects the splitting of the prime 2 in $\mathbb{Z}[(1 + \sqrt{33})/2]$. The traces of both curves modulo small primes match the coefficients of a tabulated modular form of weight 2 of level $1296 = 2^4 3^4$.

Some other examples:

For $D = 24$, we start from a surface with $L_E = R = A_3 \oplus E_6 \oplus E_7$, from which we reach the desired $U \oplus E_7 \oplus E_8$ form in a single step:



We may then exhibit $Y_-(24)$ for instance as the elliptic K3 surface over the r-line with equation

$$y^2 \;=\; -x^4 + (9r^2+2)x^3 - (24r^4 - 25r^2)x^2 \\ + (16r^6 - 36r^4 + 22r^2 - 2)x + (r^2-1)^2$$

(there's a section $(x,y) = (0, r^2-1)$). The involution ι takes y to $-y$, and again there is an involution $(x,r,y) \longleftrightarrow (x,-r,y)$ that commutes with ι and corresponds to an element of order 2 in the ideal class group of the RM ring, here $\mathbb{Z}[\sqrt{6}\,]$. This K3 surface, too, is "singular", this time with disc $\mathrm{NS}_{\bar{\mathbb{Q}}}(Y_-(24)) = -96$. The rational points $(x,r,y) = (1, \pm 3/2, \pm 9/4)$ yield the genus-2 curves

$$Y^2 = 9X^6 + 9X^4 - 60X^3 - 45X^2 + 132X - 53,$$
$$Y^2 = 9X^6 - 54X^5 + 333X^4 + 912X^3 + 351X^2 - 354X - 197$$

with isogenous Jacobians and traces that match a tabulated form of level $2592 = 2^5 9^2$. (Here the sextics are irreducible but their Galois group is S_4, embedded in S_6 as a transitive odd subgroup. The second curve is singular mod 5; this is an example where C has bad reduction and $J(C)$ is smooth but factors as a product of elliptic curves.)

For $D = 40$, we get to $U \oplus E_7 \oplus E_8$ in two steps from an elliptic surface with $L_E = R = A_4 \oplus D_5 \oplus E_7$, with the intermediate surface having $R = E_7 \oplus D_8$ and a Mordell–Weil generator of canonical height 5. Here we get $Y_-(40)$ as a double cover of $\mathbb{P}^2$ by extracting the square root of the sextic

$$-8s^6 + (25r^2 - 12r)s^4 + (-26r^4 + 24r^3 + 2r^2 - 22r + 6)s^2 + (r^2-1)(3r+1)^2(r^2-2r+2).$$

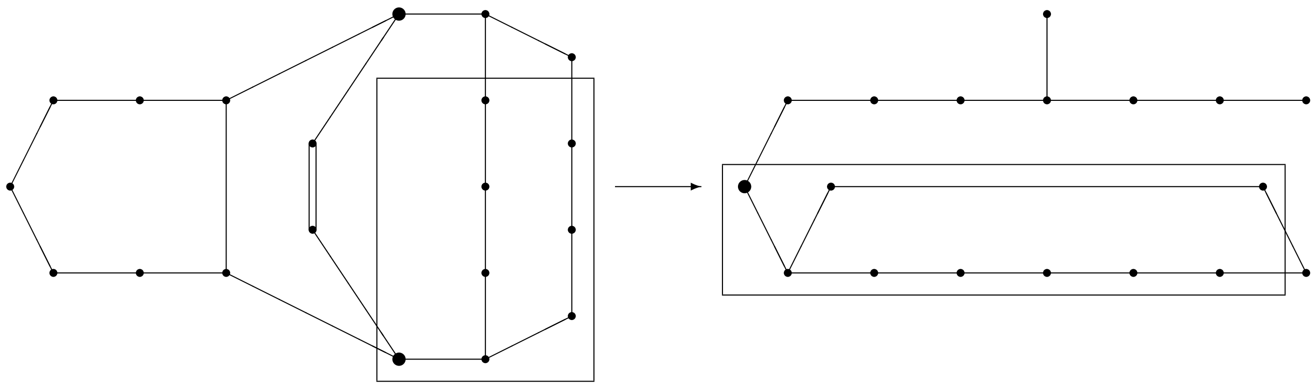
so again K3 as predicted, with the extra involution $s \longleftrightarrow -s$. Here we find only 19 independent Néron–Severi generators, and with Ronald van Luijk show that in fact $\mathrm{NS}_{\bar{\mathbb{Q}}}(Y_-(40))$ has rank "only" 19, with discriminant 168. The rational points $(r,s) = (11/8, \pm 5/8)$ yield a pair of curves

$$Y^2 = 40X^6 - 48X^5 + 77X^4 + 142X^3 + 461X^2 + 120X + 208,$$
$$Y^2 = 756X^6 - 540X^5 + 297X^4 - 986X^3 + 389X^2 - 16X + 320$$

(with irreducible sextics of discriminant $-2^{29}53^{10}$ and $-2^{23}3^{12}5^{10}$ respectively, both with Galois group S_4 and a spurious bad prime for one curve as in the $D = 24$ example above). Here we could not find the associated modular forms with coefficients in $\mathbb{Z}[\sqrt{10}\,]$ by searching the online tables.

Finally we report on $D = 53$. Here there is of course no way to start from a surface with $L_E = R$, or even with R of finite index in L_E, because no root lattice of rank 16 can have discriminant divisible by 53. (This is not the first time this happens: already for $D = 13$ there is no surface with $[L_E : R] < \infty$.) But we can still find a suitable L_E generated by vectors of small norm. We chose $R = A_1 \oplus A_6 \oplus A_8$ (rank $1+6+8 = 15$, discriminant $2 \cdot 7 \cdot 9 = 126$), with Mordell–Weil group infinite cyclic and generated by a point of canonical height $53/126$.

The zero-section, Mordell–Weil generator, and A_n components then form the configuration of (-2) curves on the left side of the picture below, with the large circles representing the zero-section and generator in either order. The double bond links the two components of the A_1 fiber, which intersect twice. The box encloses an extended E_7 diagram. Deleting it and its neighborhood leaves an A_8 diagram, so we have an elliptic fibration whose root lattice contains $A_8 \oplus E_7$, which turns out to be all of R. The resulting diagram of (-2) curves (without a Mordell–Weil generator, which has height 53/18) is shown on the right hand of the picture. The box encloses an extended E_8 diagram whose neighborhood's complement is an E_7 diagram; using the corresponding elliptic fibration we arrive at the desired $U \oplus E_7 \oplus E_8$ form of our surface.



At the end of the day we identify $Y_-(53)$ birationally with a double cover

$$y^2 = P(r,s) = \sum_{i=0}^{4} p_i(s) r^{4-i}$$

of the (r,s) plane, where the coefficients p_i are $p_0 = -27/16$, $p_1 = (-9s^2 + 63s - 13)/2$,

$$p_2 = -16s^6 + 120s^5 - 353s^4 + 560s^3 - 599s^2 + 216s - 11,$$

$$p_3 = 8s(18s^6 - 143s^5 + 458s^4 - 781s^3 + 779s^2 - 380s + 63),$$

$$p_4 = 16(s^2 - s)(-27s^6 + 207s^5 - 634s^4 + 1002s^3 - 855s^2 + 323s - 44),$$

and $\iota : (r,s,y) \longleftrightarrow (r,s,-y)$. This is a genus-1 curve over $\mathbb{Q}(s)$, with sections over $\bar{\mathbb{Q}}$ (take $r = \infty$) but apparently not over $\mathbb{Q}$. Still there is a Zariski-dense set of rational points, because $P(4,s) = -(s-1)^2(s-2)^3(3s-2)^3$, so we have a rational "quadratic section" over $\mathbb{Q}$: a rational curve on $Y_-(53)$ on which s is a function of degree 2, with the preimage of a generic s nontorsion on its genus-1 curve. There are also rational points other than those obtained from this section, such as $(r,s,y) = (141/32, 19/16, \pm 7293/2^{15})$ and $(r,s,y) = (115/32, 29/16, \pm 53^2 13/2^{15})$, which give the two examples of this RM exhibited in the introduction.

For each of our curves C with a RM Jacobian, we could even recover an endomorphism generating the endomorphism ring of $J(C)$ as an explicit correspondence on C by keeping track of the full Néron–Severi group of the various K3 surfaces arising in our construction through the chain of transformations and maps relating them. But such a computation would still be unpleasant enough that we would need a really good reason to carry it out…

Warning: we still cannot claim the existence of infinitely many ppas with real multiplication by $\mathbb{Z}[1+\sqrt{53}]/2$ over $\mathbb{Q}$ that are pairwise non-isomorphic over $\bar{\mathbb{Q}}$. Ditto for the other cases where we birationally identify $Y_-(D)$ with a surface whose $\mathbb{Q}$-rational points are Zariski-dense. This is because a K-rational point on $\mathcal{A}_2$ does not represent a ppas defined over K unless an obstruction in $\mathrm{Br}(K)[2]$ vanishes. (This phenomenon does not arise for the j-line $\mathcal{A}_1$, though it is already seen for some modular curves such as $X_0(N)/w_N$ that parametrize elliptic K-curves.) This obstruction may vanish identically on $Y_-(D)$ (this is known to happen for $D = 5$), but it does not have to, and indeed for some values of D one readily finds nontrivial obstructions over $\mathbb{Q}$. It seems reasonable to guess that some values of D, such as 29 and 53, are under-represented in the tables of modular forms because of this obstruction — or perhaps one should say that the other D's are *over*-represented because the obstruction vanishes identically on those $Y_-(D)$'s.

As hinted in the beginning, this is work in progress; $D = 53$ is just the latest case completed. It should certainly be feasible to do all the cases where $Y_-(D)$ is not of general type and the first few cases of general type, and probably also to check in each case whether the Brauer obstruction vanishes identically, and if it does to exhibit a universal genus-2 curve over (an open set in) $Y_-(D)$. Still, the modular form tables contain values of D as large as 201, and it will likely be a long time before I exhibit *that* moduli space explicitly. . .

Acknowledgements. This report is based on talks I gave at the June 2007 workshop 07w5065 at BIRS (Banff) on "Modular Forms: Arithmetic and Computation", organizer by John Cremona, Henri Darmon, Kenneth Ribet, Romyar Sharifi, and William Stein; and at the July 2007 workshop at Jacobs Univerity, Bremen on "Rational Points on Curves — Explicit Methods", organized by Michael Stoll. I thank the organizers for inviting me to give these talks, and BIRS and JU-Bremen for their hospitality during the respective workshop, the latter of which was also where Ronald van Luijk and I collaborated on the computation of $\mathrm{NS}_{\bar{\mathbb{Q}}}(Y_-(40))$. I also thank Matthias Schütt for comments and corrections on an earlier draft of this paper.

This work is based on research supported in part by the National Science Foundation through grant DMS-501029.

[Sorry, no **References** for now]