COMPUTING ISOGENIES OF ELLIPTIC CURVES

JOHN E. CREMONA AND MARK WATKINS

Abstract. October 4, 2005

1. Introduction

Let E be an elliptic curve defined over a field K. A K-isogeny of E is a map of finite degree from E to another elliptic curve E' that is also defined over K. We shall largely be interested in isogenies that have prime degree l, as one can decompose cyclic isogenies of composite degree into these. We review various methods for computing isogenous curves to and isogenies of a given curve, and introduce a slight variant upon previous methods. We also use our methodology to determine when an isogeny is étale. We conclude by describing l-isogenies in characteristic l.

Over a subfield of the complex numbers, isogenous curves can be computed using the Weierstrass parametrisation of the elliptic curve. To an elliptic curve E corresponds a fundamental lattice generated by linearly independent periods ω_1 and ω_2, and to determine curves that are l-isogenous to E we take the lattices that have index l in Λ, and invert the Weierstrass map to obtain an elliptic curve. We will always get $(l+1)$ curves (one for each subgroup of index l) that are l-isogenous over $\mathbf{C}$ to our given curve, but these need not be defined over the base field of the curve. We can, however, use complex-number approximations from this method in conjunction with techniques of detecting algebraic numbers to recover isogenous curves over a number field. Over the rationals this is particularly easy, as we can arrange for the invariants of the elliptic curve to be integral. However, this method is completely useless over, say, finite fields.

Another method to compute isogenous curves is to use the division polynomials. For an odd prime l, this is the polynomial of degree $(l^2-1)/2$ whose roots are the x-coordinates of the points of order l for a suitable Weierstrass model of the curve (with slight differences when the characteristic of the base field is 2 or 3). Via a formula of Vélu [Ve], from a suitable factor of degree $(l-1)/2$ of this division polynomial we obtain directly both an l-isogenous curve E' and an explicit isogeny from E to E'. Indeed, the kernel of this isogeny is exactly given by the point at infinity and the points whose x-coordinates are roots of this factor of degree $(l-1)/2$.

Finally there are methods based upon j-invariants. These come from the fact that the modular curve $X_0(l)$ parametrises l-isogenies, and the function field of this modular curve is generated by pairs $(j_E, j_{E'})$ that satisfy an irreducible polynomial $\Phi_l(j_E, j_{E'}) = 0$. Section 3 of the work of Elkies [E] describes this approach. Since the j-invariant only determines curves up to twist, one must first determine the correct quadratic twist of the isogenous j-invariant. Using power sums of the x-coordinates, one can then compute the kernel of the isogeny using a recursive method. Although Elkies mentions in footnote 19 on page 46 that the method fails when the degree of the isogeny sufficiently exceeds the characteristic of the field, the results we obtain here for $l = 2, 3, 5, 7, 13$ could presumably be obtained via his methods by first computing in characteristic zero and then reducing. While the method of Elkies can in theory be used for any l, one appears to need a good model for $X_0(l)$ to make it work, which is not always feasible.

There are two goals to our method; the first is practical, to push as much of the work into a pre-computation, and the second is theoretical, to replace much of the analytic elements (such as q-expansions) in the work of Elkies with algebra. Our method will be most useful for $l = 2, 3, 5, 7, 13$. While we could presumably imitate the computation of an explicit 11-isogeny given by Elkies, we see little gain in doing so. The main thrust of our method is that we obtain a completely explicit formula for the isogeny, in terms only of the j-invariant and the twisting factor, into which we can directly plug the parameters of a given curve. The major time cost in our algorithm is in the computation of the roots of a degree-$(l+1)$ polynomial that comes from the parametrisation of $X_0(l)$. From a root of this polynomial, we calculate the twisting factor and then from these data our formula immediately gives us the isogenous curve and also the polynomial of degree $(l-1)/2$ of above that records the x-coordinates of the kernel of the isogeny. So, compared to the second method of above, we need only find K-rational roots of a polynomial of degree $(l+1)$ instead of finding a factor of degree $(l-1)/2$ of a polynomial of degree $(l^2-1)/2$; this is of no significance when $l = 3$, but is much superior when $l = 13$.

As a byproduct of our explicit formulae, we are able to determine without much effort when an isogeny over a suitable field is étale. Over the rationals, this is equivalent to a determination of which isogenous curve has smaller Faltings height (larger area of fundamental parallelogram). From this we are able to classify and parametrise various families of rational elliptic curves, such as those with three étale 2-isogenies or two étale 3-isogenies, and we can also show that there is no rational elliptic curve with two étale 5-isogenies. Presumably these could be derived via other methods; our description of isogenies implies the results after a routine computation.

For many of the computations below we used the computer algebra package `Magma`, which is produced and distributed by the Computational Algebra Group within the School of Mathematics and Statistics of the University of Sydney.

2. Preliminaries

2.1. **Elliptic Curves, Models, and t-parameters.** In many of our results we shall describe models for elliptic curves as $y^2 = x^3 + f(t)U^2x + g(t)U^3$ where t and U are parameters and f and g are functions depending on the situation. A fixed value of t corresponds to a family of elliptic curve quadratic twists (all with the same j-invariant), a fixed value of t and a value of U up to squares defines an elliptic curve, and a (t, U)-pair defines a model. Note that twisting by a square value of U is what might usually be termed scaling rather than twisting. Since the parametrisations of $X_0(l)$ are given in terms of j-invariants, we most naturally get families of quadratic twists from them. In particular, every curve/model in a quadratic twist family will have the same isogeny structure. An isogeny between elliptic curves E and F descends to an isogeny between any two models M of E and N of F.

2.2. **Normalised isogenies.** Suppose that E is an elliptic curve, and let ω be a nonzero differential on E. Note that multiplying the (x, y)-coordinates of E by (λ^2, λ^3) sends ω to ω/λ, and so a model for E can be described as a pair (E, ω). Elkies [E] defines an isogeny between models $\phi : (E, \omega) \to (E', \omega')$ to be **normalised** when $\omega = \phi^\star\omega'$ (see also [G]). Given an elliptic curve isogeny from E to E' and a choice of model M for E, there is exactly one model M' of E' for which there is a normalised isogeny between M and M'; we shall refer to M' as the normalised isogenous model (to M). The normalised form of the multiplication-by-l isogeny from a curve to itself sends ω to ω/l. An isogeny is normalised if and only if its dual is also.

2.3. **Étale isogenies.** Now suppose that the field K over which E is defined is either local or global. Let (E, ω) be a model, and let (E, ω_v) be a locally minimal model at a given place v of K. We define the **distance from minimality** of (E, ω) to be

$$d_v(E, \omega) = \frac{1}{12}\big[v(\Delta(E, \omega)) - v(\Delta(E, \omega_v))\big],$$

where Δ is the discriminant for the given model. An isogeny is said to be étale at v if $d_v(E, \omega) = d_v(E', \omega')$. In particular, if (E, ω) is locally minimal at v, then an étale isogeny will map it to a model (E', ω') that is also locally minimal at v. It is can be verified that this is equivalent to the alternative definitions given by Stevens [St], namely that ϕ is étale when $\phi^\star : H^0(E'_R, \Omega^1) \to H^0(E_R, \Omega^1)$ is an isomorphism, where here R is the ring of integers of K, or that an isogeny is étale when its extension to Néron models is étale. A normalised l-isogeny ϕ is étale at places v that do not divide l, and so to check whether a normalised l-isogeny over a global field is étale, we thus need only check whether it is étale at all places that divide l.

Note that if we have an étale isogeny between models M and M' and we scale both M and M' by the same factor λ, then the resulting induced isogeny is still étale; however, this need not be true if we take the quadratic twists of M and M' corresponding to $\sqrt{\lambda}$. We can also note that over the rationals, the minimal models M and M' of l-isogenous curves E and E' have fundamental volumes that differ by a factor of l. It turns out that the isogeny $\phi : M \to M'$ is normalised, and that M has the larger volume exactly when this isogeny is étale.

3. Computations

Let E be an elliptic curve over a field K. We shall first assume that K does not have characteristic 2 or 3, and then later describe the necessary modifications needed in those cases. Under this assumption, there is a Weierstrass model for E given by $y^2 = x^3 - 27Ax - 54B$ where $c_4 = 6^4A$ and $c_6 = 6^6B$ are canonical invariants for the model. We will describe all our results in terms of such models. The lack of minimality of this model will not be that important. We could use $y^2 = x^3 - (c_4/54)x - c_6/864$ instead, but we chose to make all the constants in our results be integral. We also exclude curves with $j = 0, 1728$ at this time, and thus A and B are both nonzero.

3.1. **2-isogenies.** We start with the case of 2-isogenies, first giving our algorithm and then describing why it works. Let $M : y^2 = x^3 - 27Ax - 54B$ be a model of an elliptic curve E over a field K with $\mathrm{char}(K) \neq 2, 3$ and $j(E) \neq 0, 1728$. Find all roots $t \in K$ of $F_2(t) = (t+16)^3/t = j(E)$. For each root t let $U = \frac{(t+16)B}{(t-8)(t+64)A}$ and define $t' = 2^{12}/t$ and $U' = -Ut/2^5$. The normalised isogenous model M' is then given by $A' = (t'+16)(t'+64)U'^2 = (t+64)(t+256)U^2$ and $B' = (t'-8)(t'+64)^2U'^3 = (t-512)(t+64)^2U^3$. Writing $G(t) = (t+64)$, the normalised isogeny sends (x, y) to

$$\left(\frac{x^2 + 3xUG(t) + 1296U^2G(t)}{x + 3UG(t)}, y\frac{x^2 + 6UxG(t) + 9T^2(t-80)G(t)}{(x + 3UG(t))^2}\right)$$

and the kernel is the point at infinity and $\big(-3UG(t), 0\big) = \big(-3U(t+64), 0\big)$.

We now describe how this algorithm can be obtained. From the work of Fricke [F], one has a parametrisation of the genus zero curve $X_0(2)$ such that $j = F_2(t) = (t+16)^3/t$.[1] Using this parametrisation, we obtain an elliptic curve with this j-invariant as $y^2 = x^3 - 3j/(j-1728)x - 2j/(j-1728)$. Up to a quadratic twisting parameter U this determines A and B, and we get that $A_2(t, U) = (t+16)(t+64)U^2$ and $B_2(t, U) = (t-8)(t+64)^2U^3$. As indicated in the above algorithmic description, given values of t, A_2, and B_2 we can compute U. The linear factor of the 2-division polynomial from which we can compute the isogeny from the formula of Vélu [Ve], turns out to be $X + (192 + 3t)U$. We can compute this explicitly using `Magma` with the commands[2]

[1] THIS CAN BE OBTAINED COMPLETELY ALGEBRAICALLY??!

[2] We could simplify this somewhat by first showing that the desired factor of the division polynomial is homogeneous in X and U, and then work in a function field of one variable.

```
F<t,U>:=FunctionField(Rationals(),2);
A:=(t+16)*(t+64)*U^2; B:=(t-8)*(t+64)^2*U^3;
M:=EllipticCurve([-27*A,-54*B]);
D<X>:=DivisionPolynomial(M,2);
FAC:=Factorization(D)[1][1];
```

and then we can determine the isogeny explicitly by using the command `IsogenyFromKernel(E,FAC);` which gives the normalised isogeny using the work of Vélu.[3] However, over some fields this command may return a globally minimal model for the isogenous curve if this is possible.

Below, we do a similar computation for $l = 3, 5, 7, 13$ to get the desired factor of degree $(l-1)/2$; this involves factoring a division polynomial of degree $(l^2-1)/2$, but after we have done this once over the function field, we need not factor such a high-degree polynomial again. For $l = 13$ the calculation takes a few minutes, but as we need do it only one time, this is not a major problem.

The isogenous curve E' has $t' = 2^{12}/t$, as can be obtained from the computation of above (using the formula of Vélu), or alternatively via consideration of the action of the Fricke involution on $X_0(2)$. We can similarly compute the twisting factor U' of the isogenous curve, though it is only defined up to squares. However, in order for our isogeny to be normalised, we need the twisting factor for M' to be $-Ut/2^5$, that is, the isogeny should take the model with parameters (t, U) to the model with parameters $(2^{12}/t, -Ut/2^5)$. From this we find that the 2-isogenous model M' has $A' = (t+64)(t+256)U^2$ and $B' = (t-512)(t+64)^2U^3$.

Using our definition of normalisation that we should have $\omega = \phi^\star\omega'$, we can use `Magma` to compute that $-Ut/2^5$ is the correct choice of twisting parameter in order to normalise the 2-isogeny.

```
Ep,m:=IsogenyFromKernel(E,FAC);
Ef<X1,Y1>:=FunctionField(E); Epf<X2,Y2>:=FunctionField(Ep);
om:=BasisOfDifferentialsFirstKind(Ef)[1];
PB:=Pullback(m,BasisOfDifferentialsFirstKind(Epf)[1]);
PB eq om; // Pullback currently fails!
```

Here we must know that `BasisOfDifferentialsFirstKind` will always always return dX/Y for our curves; then the fact that the last command returns `true` implies that the isogeny obtained from `IsogenyFromKernel` is indeed normalised, as might be expected from a mechanical implementation of Vélu's formulae. From this it is a simple determination using the equation of M' to conclude that $-Ut/2^5$ is the desired twisting factor.

We can now determine when a 2-isogeny over $\mathbf{Q}$ will be étale. Recall that a normalised 2-isogeny is étale exactly when it preserves the distance to minimality at 2. A computation using the conditions of Connell [Co] regarding when a pair (c_4, c_6) is minimal, we derive that a 2-isogeny over $\mathbf{Q}$ is étale exactly when its parameters (t, U) satisfy one of:

[3]Note that the isogenies written down by Vélu are in fact normalised, as is noted in [Ve].

(1) $v_2(t) \le 4$,
(2) $v_2(t) = 5$ with $v_2(U)$ even,
(3) $v_2(t) = 6$ with $v_2(U)$ even and $v_2(t+64) \equiv 0, 1 \pmod 4$,
(4) $v_2(t) = 6$ with $v_2(U)$ odd and $v_2(t+64) \equiv 2, 3 \pmod 4$,
(5) $v_2(t) = 7$ with $v_2(U)$ odd.

The reader should be alert to the fact that a (t, U)-pair defines an isogeny, but that we shall also refer to the (t, U)-pair as corresponding to the elliptic curve and/or model that is the domain of this isogeny.

Suppose that a curve has three 2-isogenies; since the isogeny structure is constant on the quadratic twist family, we can equivalently phrase this as supposing that a t-parameter has three 2-isogenies. We can parametrise this by looking for t-values for which $F_2(x) = F_2(t)$ has 3 roots. From the quadratic formula we find that this is equivalent to $t(t+64)$ being square, so that we can write $t = 64/(u^2-1)$, with the other roots being $8(u-1)^2/(u+1)$ and $-8(u+1)^2/(u-1)$. These three roots are preserved by the transformations $u \to -u$ and $u \to 1 + 4/(u-1)$. Note that real values of t with $-64 < t < 0$ correspond to E with negative discriminant, and indeed by examination of the period lattice one can readily verify that no such curve can have three 2-isogenies over $\mathbf{Q}$.

Suppose further that we have a (model of a) rational elliptic curve E with three étale 2-isogenies. The above implies that each of the three t-parameters must have a 2-valuation of at most 7. The three t-values are all roots of $F_2(t) = E_j$, so that $(t+16)^3 = tE_j$ for each; via the formulae of Newton this implies that the sum of the t's is -48 and their product is -2^{12}. From this information and that of the previous paragraph concerning the three roots in terms of the parameter u, we compute that, up to a transformation of roots as above, we have $v_2(t) \le 7$ for all three t-values exactly when $v_2(u-1) = v_2(u+1) = 0$, so that $v_2(u) \ge 1$. We conclude that all rational elliptic curves with three étale 2-isogenies can be parametrised by taking u positive and even and $t = 64/(u^2-1)$, and then choosing $v_2(U)$ even or odd depending on the value of $v_2(t+64) = 6 + 2v_2(u)$. A computation shows that these curves are precisely those that have three rational 2-isogenies and have 2^5 exactly dividing their conductor (including the exceptional $j = 1728$ case that we have not yet described). We can also note that a similar argument shows that no rational elliptic curve can have two non-étale 2-isogenies; indeed, this is essentially implied by the theorem of Stevens [St] that states that the curve of minimal Faltings height in an isogeny class over $\mathbf{Q}$ is unique.

Note that neither an isogeny nor its dual need be étale in general. We recall Example 5 on page 41 of [Cr], where over the Gaussian field we have a minimal model M with $(c_4, c_6) = (-32, 224)$ corresponding to the pair $(t, U) = (-48, -1/4)$ and the 2-isogenous minimal model N for which we have $(c_4, c_6) = (-52, 280i)$ and $(t, U) = (-256/3, 3i/16)$. Neither isogeny is étale at $(1+i)$; the normalised isogenies take $(-48, -1/4) \to (-256/3, -3/8)$

and $(-256/3, 3i/16) \to (-48, i/2)$. At the level of differentials, if we write ω_M for a Néron differential (which is only defined up to units), we have $H^0(M_{\mathbf{Z}[i]}, \Omega^1) = \mathbf{Z}[i] \cdot \omega_M$ and similarly with ω_N. The normalised isogeny $\phi : M \to N$ has $\phi^\star \omega_N = (1+i)\omega_M$ (fixing a unit choice) and similarly $\hat{\phi}^\star \omega_M = (1-i)\omega_N$, so that neither isogeny is étale. A similar phenomenon occurs for curves that are self-isogenous.

Methods to find 4-isogenies are well-known; we briefly describe a completely algebraic method. We look for t-values for which $F_2(x) = F_2(2^{12}/t)$ has 3 roots, which is equivalent to $(t+64)$ being square. Writing $t = u^2 - 64$, the roots are $2^{12}/(u^2-64), 2^{12}(u+8)/(u-8)^2, -2^{12}(u-8)/(u+8)^2$. To obtain 8-isogenies, we can solve $F_2(x) = F_2(2^{12}(u+8)/(u-8)^2)$, and find that $u+8$ should be square. We write $u = v^2 - 8$, and another iteration of this gives that v must be square for there to be a 16-isogeny.

3.2. **3-isogenies.** Our algorithm to find 3-isogenous curves is similar. The Fricke parametrisation for $X_0(3)$ gives us that $j = F_3(t) = (t+3)^3(t+27)/t$, and thus $A_3(t,U) = (t+3)(t+27)U^2$ and $B_3(t,U) = (t+27)(t^2+18t-27)U^3$, The normalised map from one isogenous model to the other is given by $(t,U) \to (3^6/t, -Ut/3^2)$. The linear factor of the division polynomial is $X + (3t+81)U$. A computation shows that over $\mathbf{Q}$ this isogeny is étale when we have one of:

(1) $v_3(t) \le 1$,
(2) $v_3(t) = 2$ with $v_3(U)$ even,
(3) $v_3(t) = 3$ with $v_3(U)$ even and $v_3(t+27) \equiv 0,1,2 \bmod 6$,
(4) $v_3(t) = 3$ with $v_3(U)$ odd and $v_3(t+27) \equiv 3,4,5 \bmod 6$,
(5) $v_3(t) = 4$ with $v_3(U)$ odd.

We now analyse t-parameters that have (at least) two 3-isogenies. We write p, q, ξ_1, ξ_2 for the roots of $F_3(t) = j(E)$, and via the formulae of Newton are led to solve the system of equation given by the t^3, t^2, t^0-coefficients:

$$\begin{aligned} p+q+\xi_1+\xi_2 &= -36 \\ pq+(p+q)(\xi_1+\xi_2)+\xi_1\xi_2 &= 270 \\ pq\xi_1\xi_2 &= 729. \end{aligned}$$

We eliminate ξ_1 and ξ_2 by substitution of the first and second equations into the third, and are left with a genus zero curve in p and q. We shall have a similar curve when analysing 5-isogenies, and so describe how to parametrise this using `Magma` commands.

```
F<p,q>:=AffineSpace(Rationals(),2);
EQ:=q*p^3+(q^2+36*q)*p^2+(q^3+36*q^2+270*q)*p-729;
C:=ProjectiveClosure(Curve(F,EQ));
P1<x,y>:=ProjectiveSpace(Rationals(),1);
P:=Parametrization(P1,C,C![1,0,0]);
```

This gives us a parametrisation (upon simplification of the result)

$$p = \frac{3^3}{u(u^2+3u+3)} \qquad \text{and} \qquad q = \frac{3u^3}{u^2+3u+3}.$$

We can note that ξ_1 and ξ_2 will yield K-rational isogenies when the discriminant $(36+p+q)^2 - 4\cdot(729/pq) = -27\bigl(\frac{u^4+4u^3-12u-9}{u^3+3u^2+3u}\bigr)^2$ is square; thus[4] a curve that has two 3-isogenies over K has four 3-isogenies over K if and only if -3 is a square in K. In this context, letting $\rho = (1+\sqrt{-3})/2$, we can note that in Example 4 on page 41 of [Cr] the model defined over $\mathbf{Q}(\rho)$ labelled B corresponds to $u = -9, -1/3, 8\rho-1, -8\rho+7$ and

$$\begin{aligned}(t,U) =&(-1/19, 19\rho/8), \bigl((416\rho-185)/19, -(\rho+11)/14\bigr),\\ &(-729/19, 19\rho/18), \bigl((-416\rho+231)/19, (-12\rho+11)/14\bigr).\end{aligned}$$

In order for a rational elliptic curve to have two étale 3-isogenies, both p and q must have 3-valuation of at most 4, which implies that we have $v_3(u) = 0, 1$. In the first case we have $v_2(p) = 3$ and $v_2(q) = 1$, and in the second case we have $v_3(p) = 1$ and $v_3(q) = 3$; in either case we can choose the parity of $v_3(U)$ depending on $v_3(t+27) = 3v_3(U+3)$ so that the above conditions are met. A computation shows that these are, up to a twist by 3, the models with two 3-isogenies whose conductor is exactly divisible by 3^3. For example, the model $[1,-1,1,1,-1]$ numbered 54B1 by Cremona has two étale 3-isogenies, but its twist by -3, which is 54A1 given by $[1,-1,0,12,8]$, has two 3-isogenies of which only one is étale.

As we have a 3-isogeny over K, we could be interested in whether we have K-rational 3-torsion. Since the x-coordinates of the kernel of the 3-isogeny are K-rational, the K-rationality of the torsion points is determined by the twisting parameter. For instance, over $\mathbf{Q}$ for each t there is up to squares exactly one choice of U for which $x = -(3t+81)U$ makes y rational in the equation $y^2 = x^3 - 27Ax - 54B$.

We can also consider t-parameters that have both a 2-isogeny and a 3-isogeny, that is, to parametrise $X_0(6)$. Again we strive to do this in a completely algebraic way. We want $F_3(t_3) = \frac{(t_3+3)^3(t_3+27)}{t_3} = \frac{(t_2+16)^3}{t_2} = F_2(t_2)$; using `Magma` to parametrise this genus zero curve we find that

$$t_2 = -\frac{16(u_6+1)^3(u_6+5)}{2u_6+1} \quad \text{and} \quad t_3 = \frac{(2u_6+1)^2(u_6+5)}{u_6+1}.$$

In a similar manner, 12-isogenies come from taking $u_4^2 = t_2+64$ and solving $F_3(t_3) = F_2(t_2)$, which leads to an equation for $X_0(12)$ with

$$u_4 = \frac{8(v_{12}^4+36v_{12}^3+288v_{12}^2+864v_{12}+864)}{v_{12}^3(v_{12}+4)},\ t_3 = \frac{729(v_{12}+2)(v_{12}+4)^4}{v_{12}^4(v_{12}+3)(v_{12}+6)}.$$

To analyse 9-isogenies we apply the isogeny map to the above parametrisation of curves with two 3-isogenies, and get that $X_0(9)$ comes from the

[4] This also follows from a consideration of the Galois representation on $E[3]$ which is diagonal in the case we have here.

parametrisation $t_3 = 729/p = 27u_9(u_9^2 + 3u_9 + 3)$. Finally, for $X_0(18)$ we solve $F_3(t_3) = F_2(t_2)$ with this value of t_3; the fast resultant algorithms of `Magma` solve this in a few seconds, getting that

$$t_2 = \frac{(u_{18} - 2)(u_{18} + 2)^9(7u_{18}^2 + 8u_{18} + 4)}{2u_{18}^9(u_{18} + 1)(u_{18}^2 + 2u_{18} + 4)},\ u_9 = \frac{4(u_{18} - 2)(u_{18} + 1)^2}{3u_{18}(u_{18} + 2)}.$$

3.3. **5-isogenies.** For 5-isogenies the Fricke parametrisation for $X_0(5)$ is $j = F_5(t) = (t^2+10t+5)^3/t$ and $A_5(t,U) = (t^2 + 10t + 5)(t^2 + 22t + 125)U^2$ and $B_5(t,U) = (t^2 + 4t - 1)(t^2 + 22t + 125)^2U^3$. The normalised map between isogenous models is computed to be $(t,U) \to (5^3/t, -Ut^2/5^2)$, and over $\mathbf{Q}$ this isogeny is étale when $v_5(t) \le 0$, when $v_5(t) = 1$ with $v_5(U)$ even, and when $v_5(t) = 2$ with $v_5(U)$ odd.

Using `Magma` we compute that the quadratic factor of the division polynomial is given by $X^2+6(t^2+22t+125)XU+9(t^2+22t+89)(t^2+22t+125)U^2$. Note that this has discriminant $1296(t^2+22t+125)U^2$, and so factors when $t^2+22t+125$ is square. When this occurs, upon choosing U in an appropriate square class we get torsion points of order 5.

By imitating the above analysis of curves with two 3-isogenies (with four unspecified roots rather than two), we find that t-parameters with two 5-isogenies can be parametrised as

$$p = \frac{u^5}{u^4 + 5u^3 + 15u^2 + 25u + 25},\ q = \frac{5^3}{u(u^4 + 5u^3 + 15u^2 + 25u + 25)}.$$

In particular, since at least one of p and q has 5-valuation greater than 2, we see that no rational elliptic curve has two étale 5-isogenies. When a curve has at least three 5-isogenies, by looking at the representation on $E[5]$ we see that it in fact has six 5-isogenies. Since $X(5)$ has genus zero, there is a rational parametrisation of this happenstance, and a calculation shows that, similar to the case with 3-isogenies, a t-parameter with at least two 5-isogenies has six 5-isogenies precisely when 5 and $\frac{\sqrt{5}-5}{2}(u^2 + 2u + 5)$ are squares in K. Explicitly, we have that $\xi = (-b \pm \sqrt{\Delta})/2a$ where

$$b = \left(\frac{1+\sqrt{5}}{2}\right)u\left(u^2 + \frac{5-\sqrt{5}}{2}u + 5\right)\left(u^2 + (5+\sqrt{5})u + 5\right)\times$$
$$\times\left(u^4 + (5\sqrt{5}-5)u^3 + (10\sqrt{5}-5)u^2 + (25\sqrt{5}-25)u + 25\right)$$
$$a = u^2\left(u^2 + \frac{5-\sqrt{5}}{2}u + 5\right)^2\left(u^2 + \frac{5+\sqrt{5}}{2}u + 5\right),$$

and

$$\Delta = \left[\left(\frac{\sqrt{5}-5}{2}\right)(u^2 + 2u + 5)\right]u^2\left(u + \frac{5-\sqrt{5}}{2}\right)^2\left(u + \frac{5+\sqrt{5}}{2}\right)^2\times$$
$$\times\left(u + \sqrt{5}\right)^2\left(u^2 - \sqrt{5}u + 5\right)^2\left(u^2 - \frac{5-\sqrt{5}}{2}u + 5\right)^2.$$

As above, we can parametrise the genus zero curve $X_0(10)$ by solving $F_5(t_5) = F_2(t_2)$, which gives us that $t_2 = \frac{2^{12}u_{10}}{(u_{10}-1)^5(u_{10}-5)}$ and $t_5 = \frac{(u_{10}-5)^2u_{10}}{(u_{10}-1)^2}$. Finally, by applying our isogeny map to the above parametrisation of curves with two 5-isogenies, we find that the genus zero curve $X_0(25)$ can be parametrised by $t_5 = 5^3/q = u_{25}(u_{25}^4 + 5u_{25}^3 + 15u_{25}^2 + 25u_{25} + 25)$.

3.4. **7-isogenies.** For 7-isogenies the Fricke parametrisation of $X_0(7)$ gives us that $j = F_7(t) = (t^2+5t+1)^3(t^2+13t+49)/t$, and from this we derive that $A_7(t,U) = (t^2+5t+1)(t^2+13t+49)U^2$ and

$$B_7(t,U) = (t^2+13t+49)(t^4+14t^3+63t^2+70t-7)U^3.$$

The normalised map between isogenous models is $(t,U) \to (7^2/t, -Ut^2/7)$. This is étale over $\mathbf{Q}$ when $v_7(t) \le 0$ and when $v_7(t) = 1$ and $v_7(U)$ is even.

The cubic factor of the 7-division polynomial is

$$\begin{aligned}X^3 &+ 9(t^2+13t+49)X^2U + 27(t^2+13t+33)(t^2+13t+49)XU^2 + \\ &+ 27(t^2+13t+49)(t^4+26t^3+219t^2+778t+881)U^3.\end{aligned}$$

From the addition law on the elliptic curve, it follows that if this polynomial has a linear factor over $\mathbf{Q}$, then it factors completely. We again use `Magma` to parametrise the genus zero curve in X/U and t, and so parametrise these occurrences by taking $t = \frac{u^3-5u^2-8u-1}{u(u+1)}$.

3.5. **13-isogenies.** The Fricke parametrisation of $X_0(13)$ gives that

$$j = F_{13}(t) = (t^2+5t+13)(t^4+7t^3+20t^2+19t+1)^3/t,$$

and so by defining $P(t) = t^2+5t+13$ and $Q(t) = t^2+6t+13$ we have

$$\begin{aligned}A_{13}(t,U) &= P(t)Q(t)(t^4+7t^3+20t^2+19t+1)U^2,\\ B_{13}(t,U) &= P(t)Q(t)^2(t^6+10t^5+46t^4+108t^3+122t^2+38t-1)U^3.\end{aligned}$$

The normalised map between isogenous models is $(t,U) \to (13/t, -Ut^4/13)$, which over $\mathbf{Q}$ is étale when $v_{13}(t) \le 0$. Defining

$$R_4(t) = 5t^4+55t^3+260t^2+583t+537,$$

$$R_3(t) = 5t^6+80t^5+560t^4+2214t^3+5128t^2+6568t+3373,$$

$$\begin{aligned}R_2(t) = 5t^8 &+ 110t^7 + 1045t^6 + 5798t^5 + \\ &+ 20508t^4 + 47134t^3 + 67685t^2 + 54406t + 17581,\end{aligned}$$

$$\begin{aligned}R_1(t) = t^{10} &+ 27t^9 + 316t^8 + 2225t^7 + 10463t^6 + 34232t^5 + \\ &+ 78299t^4 + 122305t^3 + 122892t^2 + 69427t + 16005,\end{aligned}$$

and

$$\begin{aligned}R_0(t) = t^{14} &+ 38t^{13} + 649t^{12} + 6844t^{11} + 50216t^{10} + 271612t^9 + \\ &+ 1115174t^8 + 3520132t^7 + 8549270t^6 + 15812476t^5 + \\ &+ 21764840t^4 + 21384124t^3 + 13952929t^2 + 5282630t + 854569,\end{aligned}$$

the sextic factor of the 13-division polynomial is

$$\begin{aligned}X^6 &+ 18P(t)Q(t)X^5U + 27P(t)Q(t)R_4(t)X^4U^2 + \\ &+ 108P(t)Q(t)^2R_3(t)X^3U^3 + 243P(t)^2Q(t)^2R_2(t)X^2U^4 + \\ &+ 1458P(t)^2Q(t)^3R_1(t)XU^5 + 729P(t)^2Q(t)^3R_0(t)U^6\end{aligned}$$

This has discriminant $2^{60}3^{60}P(t)^{10}Q(t)^{15}U^{30}$. The fact that $X_1(13)$ has no noncuspidal rational points implies that this sextic never factors into linear terms over $\mathbf{Q}$. However, we can determine when it factors into quadratics or cubics. We again do this via purely algebraic methods; as noted to us by Elkies, one could alternatively use Tate's trick (whatever that is).

We replace X by YU in the above sextic factor and divide through by U^6, calling the resulting polynomial $f_t(Y)$. We first consider the case where this factors into irreducible cubics, say $f_t(Y) = A_t(Y)B_t(Y)$. Now the discriminant $\Delta(f_t)$ factors in terms of the resultant as $\Delta(A_t)\Delta(B_t)\mathrm{Res}(A_t, B_t)^2$. The elliptic curve group law implies that A_t and B_t must generate the same cubic field, and thus their discriminants differ by a sixth power (here we use the fact that A_t and B_t are irreducible). This implies that the discriminant of f_t is square, and so from the above discriminant formula we get that $Q(t) = t^2 + 6t + 13$ must be square. This turns out to be sufficient, and we get the parametrisation $t = (u^2 - 3u - 1)/u$.

We use a different argument to handle the case where $f_t(Y)$ factors into quadratics. We want to find roots α_t and β_t with $-S_t = \alpha_t + \beta_t$ and $M_t = \alpha_t\beta_t$ both rational functions of t. This can be parametrized by writing the sum and product of $f_t(\alpha_t)$ and $f_t(\beta_t)$ as functions of S_t and M_t. We then have two equations in the three unknowns S, M, and t, and can eliminate M using resultants. This gives a polynomial of multidegree $(36, 144)$ in (S, t) which fortunately factors, as the square of a term with multidegree $(3, 12)$, a term of multidegree $(6, 24)$, and the squares of two more terms of multidegree $(6, 24)$. The first term gives a curve of genus zero, and parametrising it tells us that $f_t(Y)$ splits into quadratics when $t = \frac{u^3-u^2-4u-1}{u(u+1)}$. As expected, the discriminants of these quadratics give models for $X_1(13)$ as $Y^2 = u^6 + 4u^5 + 6u^4 + 2u^3 + u^2 + 2u + 1 = F(u)$; indeed, we can note that $Q(t) = t^2 + 6t + 13 = \frac{F(u)}{u^2(u+1)^2}$, while $P(t) = t^2 + 5t + 13 = \frac{(u^2+u+1)^3}{u^2(u+1)^2}$. The other three terms from the factorisation all give curves of genus two that are isomorphic to $X_1(13)$.

The above two analyses of the splitting of the sextic polynomial are in some sense natural from the standpoint of representation theory. A curve that has a 13-isogeny corresponds to a matrix in $\mathbf{GL}_2(\mathbf{F}_{13})$ whose lower-left entry is zero. By extending the ground field to include the 13th roots of unity, we can ensure that this matrix is in $\mathbf{SL}_2(\mathbf{F}_{13})$ and thus sits inside a subgroup of order 156. The only proper subgroups of this which lead to a genus zero condition (note that the extension of the ground field does not change the genus) are the two we analysed above, along with quadratic extensions that come about from considerations with the y-coordinate.

3.6. **Curves for which $j = 0, 1728$.** We now describe isogenies in the cases where $j = 0, 1728$, again requiring that our field K have characteristic different from 2 and 3. When $j = 1728$ there always a 2-isogeny that sends $A \to -4A$ (with $B = 0$ for each model); this isogeny is explicitly given by $(x, y) \to \big((x^2+a)/x, y(x^2-a)/x^2\big)$ where M is given by $y^2 = x^3+ax$ and M' by $y^2 = x^3 - 4ax$. This isogeny can be seen as corresponding to the singular value $t = -64$ in the Fricke parametrisation. Indeed, by formally setting $(t+64)(t+16)U^2 = A_2(t, U) = -48a$, and thus $(t+64)U = 0 = (t+64)^2U^3$, the map previously given for 2-isogenies reduces to the above. Similarly, when $j = 0$ there is always a 3-isogeny (coming from $t = -27$) that sends $B \to -27B$ that is given by $(x, y) \to \big((x^3 + 4b)/x^2, y(x^3 - 8b)/x^3\big)$ where M is given by $y^2 = x^3 + b$ and M' by $y^2 = x^3 - 27b$. With the higher-degree isogenies there is similar behaviour, but the t-values might be in an extension field.

Other isogenies for these models can be determined via considerations of the twisting parameter. For instance, for a 2-isogeny we have that $t = -8$ and thus attempt to write $A_M = (t + 16)(t + 64)U^2 = 1728U^2$ for some $U \in K$. If we can do this, then our standard map $(t, U) \to (2^{12}/t, -Ut/2^5)$ is valid; we get a 2-isogeny for each such U. Similarly, when $j = 0$ so that $t = -16$, we want U with $B_M = (t - 8)(t + 64)^2U^3 = -55296U^3$, and these then yield 2-isogenies. The procedure is no different for isogenies of other degrees. For instance, it the case of 3-isogenies we find that $j = 0$ implies that $t = -3$, and thus $B_M = -1728U^3$; combined with the isogeny of the previous paragraph, this gives at least two 3-isogenies when B_M is a cube, and when this occurs we get four 3-isogenies precisely when K has three cube roots of unity, that is, when -3 is a square, the same criterion as before.

3.7. **Ordinary curves in characteristic 2 or 3.** We now describe the modifications necessary when the base field K has characteristic 2 or 3, first handling the ordinary case; we do not consider here the case of an l-isogeny in characteristic l. For any choice $l = 2, 3, 5, 7, 13$ we write the corresponding j-parametrisation in the form $j = F_l(t) = C_l(t)^3L_l(t)/t$ for polynomials $C_l(t)$ and $L_l(t)$. We first consider ordinary curves ($j \neq 0$) in characteristic 3. As in Appendix A of [Si] we can write such a curve as $y^2 = x^3 + a_2x^2 + a_6$ with $j = -a_2^3/a_6$. Thus for a given j our curve can be taken as $a_2 = C(t)L(t)U$ and $a_6 = -tL(t)^2U^3$, which appears to be the most useful choice of parameters. We again use `Magma` to determine the division polynomial as a function of t and U. Note that the use of `SimplifiedModel` will transform the curve computed with `IsogenyFromKernel` into the form denoted above. Writing $f_l = l^{12/(l-1)}$, which is $+1$ for $l = 2, 7, 13$ and -1 for $l = 5$, the image of the normalised map on (t, U)-pairs is given by $\bigl(f_l/t, f_l U t^{e_l}\bigr)$, where $e_l = 1, 2, 4, 6$ for $l = 2, 5, 7, 13$ respectively. The factors of the division polynomials for $l = 2, 5, 7, 13$ are respectively

$$K_2(t,U) = X + U, \qquad K_5(t,U) = X^2 - (t+1)XU + (t-1)U^2,$$

$$K_7(t,U) = X^3 - (t+1)(t-1)^2X^2U + (t+1)(t-1)^4XU^2 - (t-1)^4(t^2+t-1)U^3,$$

and

$$\begin{aligned} K_{13}(t,U) &= \\ & X^6 - (t+1)^2(t-1)(t^2+1)X^5U + (t+1)^4(t-1)(t^2+1)^2X^4U^2 \\ & - t(t+1)^4(t^7 - t^6 + t^5 + t^4 - t^3 + t^2 - t + 1)X^3U^3 \\ & + (t+1)^6(t-1)(t^2+1)(t^5 - t^4 + 1)X^2U^4 - (t+1)^{10}(t-1)(t^2+1)^2XU^5 \\ & + (t+1)^8(t^7 + t^6 + t^5 - t^4 - t^3 - t + 1)U^6. \end{aligned}$$

We can also note that $a_2' \neq 0$, and that, due to choice of our models, we have that $t^l \| a_6'$ (over the (t, U)-function-field). To determine l-isogenies of a given model $M : y^2 = x^3 + a_2x^2 + a_6$, we find all roots $t \in K$ of $F_l(t) = j(M)$, let $U = a_2/C_l(t)L_l(t)$ for each, and from these get the kernel $K_l(t, U)$ and apply Vélu's formula.

Similarly, for an ordinary curve in characteristic 2 we can write it as $y^2 + xy = x^3 + a_2x^2 + a_6$ with $j = 1/a_6$. We thus can write $a_6 = t/L_l(t)C_l(t)^3$ and $a_2 = U$, though there will not be any dependence on U. The normalised map is simply $(t, U) \to (1/t, U)$. Factors of the division polynomials for $l = 3, 5, 7, 13$ are respectively

$$K_3(t) = X + \frac{1}{(t+1)}, \qquad K_5(t) = X^2 + \frac{1}{(t+1)}X + \frac{1}{(t+1)^3},$$

$$K_7(t) = X^3 + \frac{t}{t^2+t+1}X^2 + \frac{t+1}{(t^2+t+1)^2}X + \frac{1}{(t^2+t+1)^3},$$

and

$$\begin{aligned} K_{13}(t) = X^6 &+ \frac{X^5}{(t+1)} + \frac{t(t^3+t+1)X^4}{(t+1)^3(t^2+t+1)^2} + \frac{tX^3}{(t+1)^3(t^2+t+1)^2} \\ &+ \frac{(t^4+t^3+1)X^2}{(t+1)^6(t^2+t+1)^4} + \frac{X}{(t+1)^7(t^2+t+1)^4} + \frac{1}{(t+1)^9(t^2+t+1)^6}. \end{aligned}$$

3.8. **Supersingular curves in characteristic 2 or 3.** The supersingular case when $j = 0$ is more complicated, as here the automorphism group of the curve is non-cyclic (see Appendix A of [Si]). In the case of characteristic 3, the canonical form is $y^2 = x^3 + a_4x + a_6$. First we describe the cases of self-isogenies of degrees 7 and 13. We assume that $-a_4 = A^2$ is a square, temporarily enlarging our field K if necessary. For $l = 7$ we obtain two

Vélu-compatible cubic factors $X^3 - A^2X \pm A^3 + a_6$ of the division polynomial, and from them we get 7-isogenies; for $l = 13$ we obtain two sextic factors

$$X^6 + A^2X^4 + (\pm A^3 - a_6)X^3 + A^4X^2 + (\mp A^5 + A^2a_6)X + (-A^6 \pm A^3a_6 + a_6^2)$$

that yield 13-isogenies. Each of the isogenies sends the model of the curve to itself. Thus to check for this type of self-isogeny we need only determine whether $-a_4$ is square.

For all other isogenies we assume $a_4 = A^2$ is square and $a_6 = B^3$ is a cube and possibly enlarge our constant field to contain $\mathbf{F}_{3^{12}}$. Then, in each case, the division polynomial splits into cubics, the number of which is $(l^2 - 1)/6$ for $l > 2$. We take any cubic that is not Vélu-compatible, note that it is singular and homogeneous in (X, A, B), transform it to a conic, and parametrise it. The resulting parametrisation gives models that have an l-division polynomial that splits completely; by recombining these linear factors in a Vélu-compatible manner we obtain the desired kernels.

For $l = 2$ we get that $(X : A : B)$ is parametrised by projective coordinates (u, v) as $\bigl(-uv^3 : u^4 : uv(u^2 + v^2)\bigr)$, and for $l = 5, 7, 13$ we have a parametrisation $(X : A : B) = (-su^3v - v^4 : u^3v : su^3v + u^2v^2 + v^4)$ where s has as its minimal polynomial respectively $s^4 - s^2 - 1$, one of $s^3 \pm s^2 \mp 1$, and one of the four polynomials $s^6 \pm s^5 - s^4 \pm s^3 - s^2 \pm s - 1$ and $s^6 \pm s^5 - 1$.

We attach a nonzero scaling factor λ to our point $(X : A : B)$ so that we have $A\lambda = u^3v$ and $B\lambda = su^3v + u^2v^2 + v^4$. Since $a_4 \neq 0$ we can take $u = 1$ and get $v = \sqrt{a_4}\lambda$ and $a_6\lambda^3 = (sv + v^2 + v^4)^3 = (s\sqrt{a_4}\lambda + a_4\lambda^2 + a_4^2\lambda^4)^3$. Nonzero solutions to this λ-equation then give us the desired kernels: we have that $K_5 = (\lambda X + sv + v^4)(\lambda X + s^3v + v^4)$,

$$K_7 = (\lambda X + sv + v^4)(\lambda X + s^3v + v^4)\bigl(\lambda X + (1 - s - s^3)v + v^4\bigr),$$

and

$$K_{13} = \prod_{i=0}^{5}\bigl(\lambda X - g^{\circ i}(-sv - v^4)\bigr)$$

where

$$g(Z) = \frac{Z^4 + v^2Z^2 + (s^3v^3 + v^6 + v^{12})Z + v^4}{Z^3 + v^2Z + s^3v^3 + v^6 + v^{12}}$$

is the doubling-map on the x-coordinate for the curve.

For $l = 2$ we have $A\lambda = u^4$ and $B\lambda = uv(u^2 + v^2)$ and the kernel is $X + \lambda uv^3$. We can take $u = 1$ and so $a_4\lambda^2 = 1$; we solve for v and substitute, getting that $a_6\lambda^3 = v^3(v^2 + 1)^3$, and so $a_6^{1/3}/\sqrt{a_4} = v(v^2 + 1)$. The v-solutions to this give us 2-isogenies.[5]

Finally we describe isogenies for supersingular curves in characteristic 2. Here the canonical form is $y^2 + a_3y = x^3 + a_4x + a_6$. We write $a_3^2 = B^3$ and $a_4 = A^2$, and ensure that $\mathbf{F}_{2^{12}}$ is contained in the ground field. Then for $l = 3, 5, 7, 13$ the l-division polynomial (which is independent of a_6) factors

[5]In practise, simply factorising the division polynomial may be superior.

into $(l^2-1)/8$ singular quartics, and again we can transform these into conics and parametrise them. We get that $(X : A : B)$ is

$$\big((t+1)u^8 + tu^4v^4 + v^8 : tu^8 + u^7v + (t+1)u^4v^4 + u^3v^5 + v^8 : u^4(u^4+v^4)\big)$$

where for $l = 3, 5, 7, 13$ we have that $t = 0, 1$, then satisfies $t^6 + t^3 = 1$, and satisfies $t^{12} + t^3 = 1$. We have that $\Delta = a_3^4 \neq 0$, and so we can take $u = 1$ in our projective coordinates, attaching a scaling parameter λ as we did previously. We have that $v^4 + 1 = B\lambda = a_3^{2/3}\lambda$ and plug this into $v^8+v^5+(t+1)v+v+t = A\lambda = \sqrt{a_4}\lambda$ to get an octic v-relation; the roots of this give us kernels as $K_3 = \lambda X + 1 + v^8$, $K_5 = (\lambda X + v^4 + v^8)(\lambda X + 1 + v^8)$,

$$K_7 = (\lambda X + t + 1 + tv^4 + v^8)(\lambda X + 1 + v^8)(\lambda X + t^4 + 1 + t^4v^4 + v^8),$$

and

$$K_{13} = \prod_{i=0,1,4,7,10,37} (\lambda X + t^i + 1 + t^iv^4 + v^8).$$

3.9. **Characteristic is l.** For completeness: l-isogenies when the characteristic is l. Voloch [Vo], Ulmer [U].

3.10. **Comments on cases where $X_0(l)$ is not genus zero.** ?

References

[Co] I. Connell, Lecture Notes from class at McGill University, 1991, Chapter 5. Online as the Elliptic Curve Handbook, `www.math.mcgill.ca/connell/public/ECH1/c5.ps`

[Cr] J. E. Cremona, *Periods of Cusp Forms and Elliptic Curves over Imaginary Quadratic Fields.* Elliptic Curves and Related Topics, 29–44, CRM Proceedings and Lecture Notes, 4, Amer. Math. Soc., Providence, RI, 1994.

[E] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues.* Computational perspectives on number theory (Chicago, IL, 1995), 21–76, AMS/IP Stud. Adv. Math., 7, Amer. Math. Soc., Providence, RI, 1998.

[F] R. Fricke, *Not sure which book.*

[G] J. González, *Isogenies of polyquadratic* **Q***-curves to their Galois conjugates.* Arch. Math. **77** (2001), no. 5, 383–390.

[Si] J. H. Silverman, *The arithmetic of elliptic curves.* Corrected reprint of the 1986 original. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1994.

[St] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves.* Invent. Math. **98** (1989), no. 1, 75–106.

[U] D. L. Ulmer, *p-descent in characteristic p.* Duke Math. J. **62** (1991), no. 2, 237–265.

[Ve] J. Vélu, *Isogénies entre courbes elliptiques.* (French) C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.

[Vo] J. F. Voloch, *Explicit p-descent for elliptic curves in characteristic p.* Compositio Math. **74** (1990), no. 3, 247–258.