Explicit models for modular curves.

Kevin Buzzard

February 7, 2012

Last modified 19/09/2011 (but written much much earlier).

Let E/S be an elliptic curve over a scheme. Then E/S is smooth and hence locally of finite presentation, and proper and hence quasi-compact, so it's of finite presentation. Hence one can cover S by affines U_i such that on each U_i we have $E|U_i$ is the pullback of an elliptic curve over a Noetherian ring. This is in EGA IV, sections 8 through 11 (specifically 8.9.1 and 11.2.6.1). So WLOG S is Noetherian, for what we're going to do, which is constructing explicit models for modular curves. Let $f : E \to S$ denote the structure map and let $e : S \to E$ denote the zero section. Now Lemma 1.2.2 of Katz-Mazur shows that the image of e defines what they call an effective Cartier Divisor, and its ideal sheaf is an invertible sheaf on E. Let $\mathcal{O}(e)$ denote its inverse, and let $\mathcal{O}(ne)$ denote the nth tensor power of $\mathcal{O}(e)$, $n \geq 0$. Recall Grothendieck's generalisation of the fact that cohomology of a coherent sheaf on a projective variety is finite-dimensional: if f is proper morphism between Noetherian schemes then $R^i f_*$ of a coherent sheaf is coherent. Hartshorne III.8.8(b) for the projective case, EGA III 3.2.1 for the proper case. Another standard cohomology and base change result is the following.

Theorem 0.1 (Mumford ab vars p53)**.** *If $X \to Y$ is a proper morphism and Y is affine and $\mathcal{F}$ is coherent on X and flat over Y and if, for some n we have $H^n(X_y, \mathcal{F}_y) = 0$ for all $y \in Y$, then $R^{n-1} f_* \mathcal{F}$ commutes with all base changes.*

Now we show that if $n \geq 1$ then $f_*\mathcal{O}(ne)$ is locally free of rank n and commutes with all base changes; see p66 of Katz-Mazur for the argument. The idea is that applying the theorem with $n = 2$ gives that $R^1 f_*\mathcal{O}(ne)$ is coherent and commutes with base changes, and now looking at points shows $R^1 f_*\mathcal{O}(ne) = 0$, so now applying Mumford ab vars theorem on p46 and also the lemma on p47 with $n = 0$ and the lemma on p49, we deduce that $f_*\mathcal{O}(ne)$ is locally free and commutes with all base changes.

Let's cover S by open affines over which $f_*\mathcal{O}(ne)$ is free, for $1 \leq n \leq 6$. Let $S = \mathrm{Spec}(R)$ now denote one of these affines and write M_n for $f_*\mathcal{O}(ne)$. Now the usual tricks work. There are maps $M_n \to M_{n+1}$ and the map $M_0 \to M_1$ is an isomorphism because it's true on fibres. So 1 is a basis for M_1. Let $\{1, x\}$ be a basis for M_2; such a thing exists because if R is a ring and we have an R-module homomorphism $R \to R^2$ sending 1 to (a, b) and with the property

that the ideal generated by a and b is R, then we can solve $\lambda a + \mu b = 1$ and hence extend the map $R \to R^2$ to an isomorphism $R^2 \to R^2$.

Let's normalise x slightly carefully: if we choose an isomorphism of the completion of E along e with $S[[t]]$, then we know that $x = ut^{-2} + \dots$ and u must be a unit becuase it's not contained in any maximal ideal. So WLOG $u = 1$.

Now go to M_3. If we have a 3×2 matrix over a ring and modulo every maximal ideal of this ring the matrix has rank 2, then one of the two by two minors of this matrix will be non-zero, so the ideal generated by these three minors is R, so we can extend to an invertible 3×3 matrix. So we can beef up $\{1, x\}$ to $\{1, x, y\}$, a basis of M_3. We can ensure also that $y = t^{-3} + \dots$.

Now I claim that $1, x, y, x^2, xy$ must be a basis for M_5. This is clear because they all have poles of different orders at the origin.

So because $y^2 - x^3$ is in M_5 we find a relation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

and this shows that the map $E \to \mathbf{P}^2$ defined by the very ample sheaf $\mathcal{O}(3e)$ has image lying in this cubic and for dimension reasons this must be an isomorphism, I guess.

This model is in no way unique. We chose a uniformising parameter t and unravelling we see that our degrees of freedom are given by sending $x \to u^2x + a$ and $y \to u^3y + bx + c$, with u a unit and a, b, c arbitrary. So amongst our 5 variables we have 4 ways of changing them and this is morally why modular curves are 1-dimensional.

We conclude that locally on the base, an elliptic curve is given by the usual equation above.

Now let's consider an S-valued point P of E which is not the zero section on any fibre (note that in characteristic 2 we could have a section which usually has order 2 but which suddenly has order 1 at a supersingular fibre. Terrifying!). Using the a and c freedom above, we can assume that on each of our models, P is the point $(0, 0)$. So our equation becomes

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x.$$

Now the line $x = 0$ meets the curve at infinity, $(0, 0)$ and $(0, -a_3)$. So if P hasn't got order 2 on any fibre either, then $v := a_3$ will be a unit. Now we use our b flexibility, sending y to $y - (a_4/a_3)x$, to conclude that if P isn't killed by 2 on any fibre, then we can write our curve as

$$y^2 + a_1xy + vy = x^3 + a_2x^2.$$

We still have our u flexibility, but we have gained a degree of freedom because our condition on P is morally open. Note that $-P = (0, -v)$. Let's now try the line $y = 0$; we have assumed that P doesn't have order 2 so it's no surprise to see that $-2P$ can never be infinite; we see that $-2P = (-a_2, 0)$.

So if P doesn't have order 3 on any fibre either, then a_2 is also a unit. Because a_2 is weight 2 and v is weight 3, we can finally use our u dependency and assume that $a_2 = v$ as well! Now we have no more flexibility, but we do have a conclusion: if P doesn't have order 1,2 or 3 on any fibre, then locally the curve looks like

$$y^2 + a_1xy + vy = x^3 + vx^2,$$

with $P = (0, 0)$, $-P = (0, -v)$, $-2P = (-v, 0)$, and v a unit.

Note that the lines $x = c$ all go through infinity and can be used to find the inverse of a point on the group law; the inverse of (x, y) is $(x, -a_1x - v - y)$. In particular we see that $2P = (-v, (a_1 - 1)v)$. Another one: the line through $-P$ and $-2P$ is $y = -x - v$ and substituting in and comparing terms in x^2 we see that $3P = (1-a_1, a_1-v-1)$, and $-3P = (1-a_1, (1-a_1)^2)$. *Pari is really really good for working these out;* $e = ellinit([a1, v, v, 0, 0]); P = [0, 0]; ellpow(e, P, 3)$ *for example to see things in huge generality.*

Now the results come easy. For example, $4P = 0$ iff $2P = -2P$ iff $a_1 = 1$ and we see that $Y_1(4)$ is the open subscheme of $\mathbf{A}^1$ where v is invertible and where

$$y^2 + xy + vy = x^3 + vx^2$$

is smooth. Similarly, if P has order 5 on each fibre then we want $3P = -2P$ so $a_1 = 1 + v$. Note finally that if $4P$ isn't zero then $a_1 - 1$ is a unit, maybe this helps?