

Woods Hole, fake CM, near logarithms and stable reduction.

Robert F. Coleman

The modular curve $X_0(p^n)$

Let p be a prime. For $n > 3$ the stable model of $X_0(p^n)$ is not known. When $n = 1$ it was determined by Deligne and Rapoport in 1973. When $n = 2$ it was determined by Edixhoven in 1989. When $n = 3$ ($p \neq 11$) its reduction was determined by McMurdy and myself last year.

The minimal regular model is exposed in Katz-Mazur. One sees that all the trouble comes from supersingular points.

Stable reduction of $X_0(p^3)$

Suppose $p \geq 5$.

There are 6 “ordinary” components.

In a supersingular residue class with $j \neq 0$ or 1728, there are two “too supersingular” $y^2 = x^{p+1} + 1$ components.

One genus 0 “bridging” component.

$2(p+1)$ “self-dual” $y^2 = x^p - x$ components.

Woods Hole

Suppose E is a supersingular elliptic curve over a finite field k of characteristic p and R is a complete DVR with residue field k . Then the category of pairs (A, D) where A is a lifting of E over R and D is a cyclic subgroup of order p^n is equivalent to the category of triples (C, F, α) where

F is a formal group over R ,

$\alpha: \bar{F} \rightarrow \hat{E}$ is an isomorphism and

C is a cyclic subgroup of order p^n of $F[p^n]$.

There is a rigid space $M_n(E)$ over $W_{\mathbf{Q}}(k)$ such that these points can be identified with $M_n(E)(R)$.

In particular, $\text{Aut}(\hat{E})$ acts on $M_n(E)(R)$. If $\gamma \in B =: \text{End}(\hat{E})$.

$$m_\gamma: (C, F, \alpha) \mapsto (C, F, \gamma \circ \alpha)$$

and $\mathbf{Z}_p^* \subset B^*$ acts trivially. If $k \supseteq \mathbf{F}_{p^2}$ and $-r \in \mathbf{Z}_p$ is not a square. $\text{Aut}(\hat{E}) = B^*$ where

$$B = \{a + bi + cj + dk: a, b, c, d \in \mathbf{Z}_p\}$$

$$ij = -ji = k, i^2 = -r, j^2 = -p.$$

If $A(F, \alpha)$ is the isomorphism class of elliptic curves corresponding to $(F, \alpha) \in M_0(E)$ ■
lets abusively think of $A(F, \alpha)$ as an elliptic curve. Then

$$A(\widehat{F}, \alpha) \cong F$$

.

The too supersingular and self-dual circles

We can identify $M_1(E)$ with the annulus in $X_0(p)$, $\mathcal{A}(E)$, corresponding to E and if E/\mathbf{F}_p , this annulus is fixed by w_p .

There are two concentric circles (tires) in $\mathcal{A}(E)$. Suppose for simplicity $j(E) \neq 0$ or 1728.

The too-supersingular circle, $TS := TS_E$

whose points over \mathbf{C}_p correspond to pairs (A, C) where A is too-supersingular or equivalently where the points of order p on A are equidistant or such that $E \bmod p$ has Hasse invariant of valuation $\frac{p}{p+1}$.

Eg., A has CM by an order of discrim. D with $(\frac{D}{p}) = -1$.

The self-dual circle, $SD := SD_E$

whose points correspond to pairs (A, C) where C is a self-dual group scheme or equivalently $A \bmod p$ has Hasse invariant of valuation $\frac{1}{2}$ and C is the canonical

subgroup, or A/\mathbf{F}_p and SD is the circle fixed by w_p .

Eg., A has CM by an order of discrimin. pD . $(D, p) = 1$ and C is the kernel of the prime above p .

B^* acts on these circles. $\mathbf{Z}_p^* \subset B^*$ acts trivially and

Theorem. $B^*/\mathbf{Z}_p^*(1+jB) \cong \mu_{p^2-1}/\mu_{p-1}$ acts faithfully on \overline{SD} .

The proof of this requires Honda's description of crystalline cohomology of elliptic curves in terms of **near logarithms**.

Going up to $X_0(p^3)$.

We have 3 maps $\pi_{ab}: X_0(p^3) \rightarrow X_0(p)$, $a+b=2$, $0 \leq a \leq 2$;

$$\pi_{ab}: (A, C) \mapsto (A/C[p^b], p^a C/C[p^b]).$$

It turns out that $\pi_{2,0}^{-1}TS$ and $\pi_{0,2}^{-1}TS$ are affinoids above the non-singular points of two components of the stable reduction.

Suppose now E/\mathbf{F}_p . Then we can make a lot of involutions. First, if $\rho \in \mathcal{U} := \{\sigma \in B^*: \sigma = a + bi + dk\}$, $T_\rho := \rho \circ w_p$ is an involution of SD . Using the above faithfulness result, we show these reduce to $p+1$ involutions with a total of $2(p+1)$ fixed points.

Let $\mathcal{C} := \mathcal{C}_E$, be the circle in $\mathcal{A}(E)$ whose points correspond to pairs (A, C) where $A \bmod p$ has Hasse invariant of valuation $1/2$ but C is **not** canonical and $f: \mathcal{C} \rightarrow SD$ the natural map.

Proposition. *There is an isomorphism*

$$\psi: \mathcal{S} := \{ (x, y) \in \mathcal{C} \times \mathcal{C}: f(x) = w_p \circ f(y) \} \rightarrow \mathcal{Z}$$

so that $w_{p^3}(\psi(x, y)) = \psi(y, x)$ and $\pi_{1,1}(\psi(x, y)) = f(x)$.

Using a result of de Shalit which describes how $\mathcal{A}(E)$ sits over the j -line we show that \mathcal{Z} reduces to

$$u^{2p+2} - v^p u^{p+1} + 1 \equiv 0$$

This curve has genus 0 and $2(p+1)$ singular points which lie over the fixed points of T_ρ on \overline{SD} for some $\rho \in \mathcal{U}$. It is these residue classes which contain the rest of the stable model. Let W be one of these residue classes.

Lemma. *If $\rho \in \mathcal{U}$, $\tilde{T}_\rho: (x, y) \in \mathcal{S} \mapsto (\rho y, \bar{\rho} x)$ is an involution above T_ρ . Moreover, the fixed points of \tilde{T}_ρ lie p to 1 over the fixed points of T_ρ .*

Thus \tilde{T}_ρ is an involution of W . We next make an automorphism S_ρ of order p of W which commutes with \tilde{T}_ρ and permutes the fixed points. This can all be done over $W(\overline{\mathbf{F}}_p)[p^{1/(p^2-1)p^2}]$.

Now by a genus argument W must contain an affinoid which reduces to

$$t^2 = s^p - s.$$

Real and Fake CM

If $\text{End}(\hat{A}) \neq \mathbf{Z}_p$, A is said to have **fake CM**. Eg. all supersingular curves over $W(\mathbf{F}_{p^2})$ have fake CM and are too supersingular. Also all of the previously mentioned fixed points correspond to curves with fake CM.

If $A(F, \alpha)$ has CM and if $\gamma \in B^*$, $A(F, \gamma \circ \alpha)$ has fake CM.

Also, if A lifts E and has fake CM by the ring of integers in a ramified quadratic extension of \mathbf{Q}_p and C is the kernel of the prime above p , (A, C) corresponds to a point above one of one of the self-dual components.

Theorem. *Suppose $R = W(\mathbf{F}_{p^2})[\sqrt{p}]$. Then the set of fake CM points in $SD(R)$ lie in two B^* orbits corresponding to the two ramified quadratic orders. Moreover the real CM points in $SD(R)$ are dense in the fake ones.*