

$X_0(p^2)$ and the too supersingular circle (continued)

Robert Coleman

The KME model of $X_0(p)$ is semistable and stable if $p \geq 23$. Call this model $\mathcal{X}_0(p)$ and Esikhovwen's model of $X_0(p^2)$ $\mathcal{X}_0(p^2)$

Theorem. (*Edixhoven*) *The model $\mathcal{X}_0(p^2)$ is semistable, has four vertical components and SS horizontal components (one corresponding to every supersingular point).*

IV A Rigid Point of View

A **semi-stable cover** of Y is a covering \mathcal{C} of Y by rigid opens such that if $U \neq V \in \mathcal{C}$, $U \cap V$ is a disjoint union of wide open annuli and $U^o = U - \bigcup_{V \neq U} V$ is either proper or an affinoid and has irreducible reduction with at worst ordinary double points.

If \mathcal{Y} is a semi-stable model for Y and T_i are the irreducible components of the reduction of \mathcal{Y} , $\{\text{red}^{-1}T_i\}$ is a semi-stable cover.

Let $\mathbf{Z}(s) = \text{red}^{-1}\mathbf{Z}(s) - \text{red}^{-1}(X_{20} \cup X_{11}^+ \cup X_{11}^- \cup X_{02})$.

V Annuli

A wide open annulus is a rigid space X conformal to $A(r, s) =: \{x \in \mathbf{C}_p: r < |x| < s\}$ for some $0 < r < s \in |\mathbf{C}_p|$. The width of X , $W(X)$, is $\log_p(s/r)$. If T is such a conformal map and $r, s \in |K|$.

$$A(X)^* = \{cT^n g: c \in K^*. n \in \mathbf{Z} \text{ and } |g(x) - 1| < 1 \text{ for } x \in X\}.$$

Lemma. *If $f: A \rightarrow B$ is a surjective morphism of wide open annuli then it is finite and $W(B) = \deg(f)W(A)$.*

Lemma. *Suppose $f(T)$ is a unit on $A =: A(r, 1)$. Also suppose $\sup_{x \in A} |f(x)| = 1$ and $|f(x)| < 1$ for all $x \in A$. Then $f(A) = A(s, 1)$ where $s = \inf_{x \in A} |f(x)|$.*

By a **circle**, I mean a closed annulus of width 0.

VI Canonical subgroups

If E is an elliptic curve over R with good reduction. $E[p]$ reduces to a group of order p or 1. In the former case, the reduction is said to be **ordinary**. In the latter **supersingular**. But even when E has supersingular reduction one can sometimes make a group of order p in $E[p]$ in a canonical way. When it exists it is the non-trivial cyclic subgroup of $E[p]$ closest to the origin.

Suppose (E, C) corresponds to a point on $X_0(p)$ over R . If this point reduces to a (non-cuspidal) smooth point on the reduction of $\mathcal{X}_0(p)$ E has ordinary reduction. This point lies in X_∞ if and only if C is the kernel of reduction. If this point reduces to a singular point, E has supersingulae reduction.

Let s be a singular point on the reduction of $\mathcal{X}_0(p)$, its inverse image is an annulus $A_1(s)$. When $s \neq 0, 1728$ there exist $T: A(s) \cong A(1, |p|)$ such that $|T(x)| \rightarrow 1$ as $x \rightarrow \text{red}^{-1}(X_\infty)$. Then if (E, C) corresponds to $x \in A(s)$, E has a canonical subgroup if and only if

$$v(T(x)) \neq \frac{p}{p+1}$$

(otherwise E is said to be **too supersingular**) and it is C iff

$$v((x)) < \frac{p}{p+1}.$$

Finally $v(T(x)) = 1/(p+1)$ iff

$$(E, C) = (A/D, A[p]/D)$$

for some too supersingular elliptic curve A and some subgroup of A of order p , D .

Call this circle $\mathcal{C}(s)$.

Examples.

VII Interpretation of the horizontal components

Let $\pi: X_0(p^2) \rightarrow X_0(p)$ be $(E, C) \mapsto (E, pC)$.

Theorem. $\mathbf{Z}(s) = \pi^{-1}(\mathcal{C}(s))$.

Proof. First note that π has degree p . Let $U(s) = \text{red}^{-1}\mathbf{Z}(s)$. Then

$$U(s) - \mathbf{Z}(s) = A_{20}(s) \cup A_{11}^+(s) \cup A_{11}^-(s) \cup A_{02}(s)$$

Lemma. $\pi(\mathbf{Z}(s))$ is contained in a circle.

Lemma. $W(A_{20}(s)) = W(A_{02}(s))$.

Lemma. $W(\pi(A_{20})) = W(A_{20})$ and $W(\pi(A_{02})) = pW(A_{02})$.

Lemma. $\pi(A_{02})$ doesn't intersect $\pi(A_{11}^+)$, $\pi(A_{11}^-)$ or $\pi(A_{20})$.

Corollary. $W(\pi(A_{20})) + W(\pi(A_{02}(s))) = 1$.

End of proof

VIII Vertical Components

Suppose (E, C) is a pair consisting of an elliptic curve with ordinary reduction and cyclic group of order p^2 such that $pC = K_1(E)$ but $C \neq K_2(E)$. Suppose $a, b \in K_1(E)$. Set

$$(a, b) = (\alpha, \beta)_{Weil}$$

where $\alpha \in K_2(E)$, $p\alpha = a$, $\beta \in C$ and $p\beta = b$.

Lemma. *There are two isomorphism classes of non-generate pairings on a one dimensional vector space over \mathbf{F}_p into μ_p .*

Picking a root of unity and a quadratic non-residue we get a pairing

$$\bar{E}[p] \times \bar{E}[p] \rightarrow \mathbf{F}_p$$

and hence an element up to sign of $\bar{E}[p]$.