Introduction

$p \nmid DN$

$p | N$

$p | D$

Rational Points

Twists of Shimura Curves

Jim Stankewicz

Department of Mathematics
The University of Georgia

January 5, 2012

Modular and Shimura Curves

Let N be a positive integer and k be a field. Define $Y_0(N)$ so that

$$Y_0(N)(k)\text{"} = \text{"}\{(\phi : E_1 \to E_2)_{/k}\}$$

where E_1, E_2 are elliptic curves over k and $\ker \phi$ is cyclic of order N.

By $X_0(N)$ we denote the natural compactification of $Y_0(N)$.

If B_D is a quaternion algebra over $\mathbb{Q}$ of discriminant D, $X_0^D(N)$ is the Shimura curve analogue of $X_0(N)$.

Why Shimura curves?

- Useful for studying Elliptic curves and abelian varieties
- Modular forms for $\Gamma_0(N)$ are given by the cohomology of $Y_0(N)_{\mathbb{C}}$
- Level-raising and level-lowering is given by the interplay between $X_0^D(N)$ and $X_0(DN)$.

Atkin-Lehner Involutions

$X_0^D(N)$ comes furnished with a group of automorphisms $W = \{w_m : m \| DN\}$ called the Atkin-Lehner group. If $m \neq 1$, that is $w_m \neq \mathrm{id}$, then w_m is of order two and is called an Atkin-Lehner involution.

For simplicity, we talk only about the *main* Atkin-Lehner involution w_{DN}. Note that if $D = 1$ then on $X_0^1(N) = X_0(N)$ this simply takes an isogeny $\phi : E_1 \to E_2$ to the dual isogeny $\widehat{\phi} : E_2 \to E_1$.

The Big Question

Work of Shimura shows that $X_0^D(N)_{\mathbb{C}}$ can be given the structure of a smooth variety over $\mathbb{Q}$. He also showed that $X_0^D(N)(\mathbb{Q}) \neq \emptyset$ if and only if $D = 1$.

Question: Are there any *other* ways to give $X_0^D(N)_{\mathbb{C}}$ a $\mathbb{Q}$ structure? Any for which there are $\mathbb{Q}$-rational points? For which there are *many* rational points?

The Big Question

Work of Shimura shows that $X_0^D(N)_{\mathbb{C}}$ can be given the structure of a smooth variety over $\mathbb{Q}$. He also showed that $X_0^D(N)(\mathbb{Q}) \neq \emptyset$ if and only if $D = 1$.

Question: Are there any *other* ways to give $X_0^D(N)_{\mathbb{C}}$ a $\mathbb{Q}$ structure? Any for which there are $\mathbb{Q}$-rational points? For which there are *many* rational points?

Equivalent Question: Are there any twists of $X_0^D(N)_{/\mathbb{Q}}$ which have rational points? Many rational points?

Why Atkin-Lehner twists?

- Conjecturally, $W = \mathrm{Aut}(X_0^D(N))$ for all but finitely many (D, N)
- Atkin-Lehner twists over $\mathbb{Q}$ parametrize abelian varieties over quadratic fields whose Galois representations descend down to $\mathbb{Q}$
- There is a connection between rational points on Atkin-Lehner twists and the inverse Galois problem
- The action of Atkin-Lehner on "superspecial points" in positive characteristic can be understood in terms of quaternion arithmetic.

First step: Use Hensel's Lemma along with the action on superspecial points to understand p-adic points.

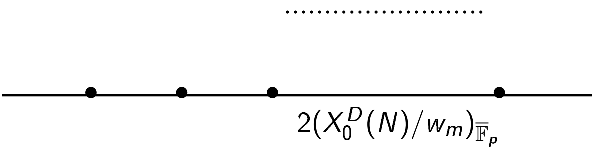
If $p \nmid DN$

Let $C^D(N,d)$ denote the twist of $X_0^D(N)$ by $\mathbb{Q}(\sqrt{d})$ and w_{DN} and suppose that no prime ramified in $\mathbb{Q}(\sqrt{d})$ divides DN.

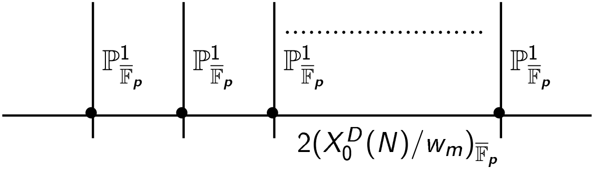
Theorem (S-)

If p is inert in $\mathbb{Q}(\sqrt{d})$, $C^D(N,d)(\mathbb{Q}_p)$ is nonempty. If $p \neq 2$ is ramified, $C^D(N,d)(\mathbb{Q}_p)$ is nonempty if and only if p has a degree one factor in $\mathbb{Q}(j(\sqrt{-DN}))$ or $\mathbb{Q}\left(j\left(\frac{1+\sqrt{-DN}}{2}\right)\right)$.

Giving a model when p is ramified



Giving a model when p is ramified



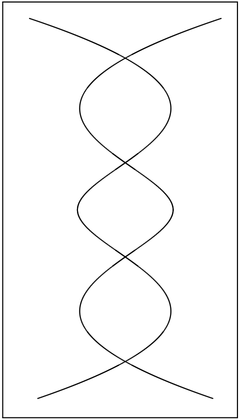
p|N

Theorem (S-)

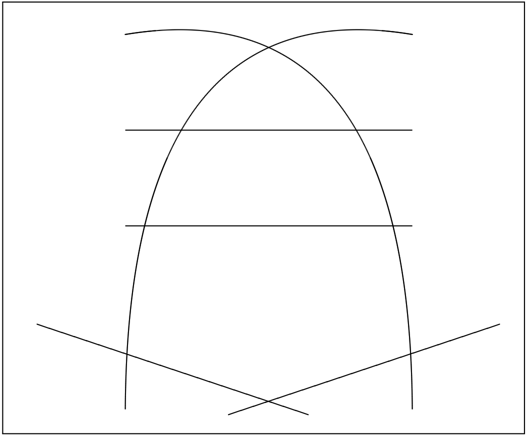
If $p|N$ is inert in $\mathbb{Q}(\sqrt{d})$ then $C^D(N,d)(\mathbb{Q}_p) \neq \emptyset$ if and only if one of the following holds:

- $p = 2$, *for all* $q|D$, $q \equiv 3 \bmod 4$, *for all* $q|(N/2)$, $q \equiv 1 \bmod 4$
- $p \equiv 3 \bmod 4$, $D = 1$, $N = p$ *or* $2p$

$X_0(39)_{\overline{\mathbb{F}}_3}$



The $\overline{\mathbb{F}}_3$ special fiber of a regular model



$p|D$

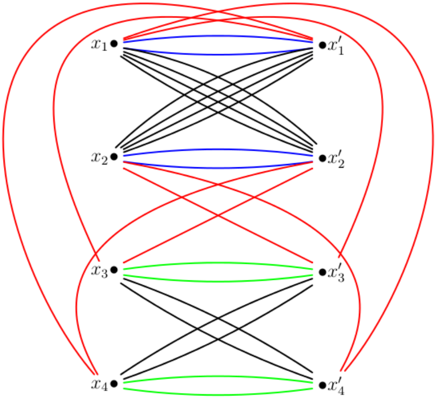
Theorem (S-)

If $p|D$ is inert in $\mathbb{Q}(\sqrt{d})$, $C^D(N,d)(\mathbb{Q}_p)$ is nonempty. If $p|D$ is split, then $C^D(N,d)(\mathbb{Q}_p)$ is nonempty if and only if

- $p = 2$ *and for all* $q|(D/2)$, $q \equiv 3 \bmod 4$, *for all* $q|N$, $q \equiv 1 \bmod 4$
- $p \equiv 1 \bmod 4$, $D = 2p$, $N = 1$

Dual graph of $X_0^{858}(1)_{\overline{\mathbb{F}}_{13}}$

Red edges correspond to fixed points of w_{66}



An Application

Corollary

If $\left(\frac{-14}{p}\right) = -1$ *then* $C^1(14, p^*)(\mathbb{Q}_v)$ *is nonempty for all places* v *of* $\mathbb{Q}$ *if and only if* $\left(\frac{2}{p}\right) = 1$, $\left(\frac{-7}{p}\right) = -1$

Corollary (Depends on the parity conjecture)

If $p \equiv 17, 33, 41 \bmod 56$, $C^1(14, p)$ *is a rank one elliptic curve.*

End

Thank you!