



Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

# Serre's Account of Shih's Theorem

Jim Stankewicz

Department of Mathematics  
The University of Georgia

September 9, 2009



Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

Today we aim to prove Shih's Result on the Inverse Galois Problem:

### Theorem (Shih, 1974)

*If  $p$  is an odd prime such that one of  $\left(\frac{2}{p}\right)$ ,  $\left(\frac{3}{p}\right)$ ,  $\left(\frac{7}{p}\right)$  is  $-1$  then there is a Galois extension  $L/\mathbf{Q}$  (in fact infinitely many) such that  $\text{Gal}(L/\mathbf{Q}) = \text{PSL}_2(\mathbf{Z}/p\mathbf{Z})$ .*



Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

Shih proved this theorem by proving the following

### Theorem (Geometric Version)

*There is a covering of curves defined over  $\mathbf{Q}$ ,  $C \rightarrow \mathbb{P}^1$  with automorphism group  $PSL_2(\mathbf{Z}/p\mathbf{Z})$  for the same list of odd primes  $p$ .*

and then using Hilbert's Irreducibility Theorem to get a field extension of  $\mathbf{Q}$ .

### Theorem (Hilbert's Irreducibility Theorem)

*If  $L_T$  is a regular Galois field extension of  $\mathbf{Q}(T)$  (one such that  $L_T \cap \overline{\mathbf{Q}} = \mathbf{Q}$ ) with Galois group  $G$  then there are infinitely many  $a \in \mathbf{Q}$  such that  $L_a/\mathbf{Q}(a)$  (note that  $\mathbf{Q}(a) = \mathbf{Q}$ ) is a Galois extension with Galois group  $G$ .*

For a proof, see [Serre, Chapter 4].



# A Foundational Result

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

The following works for a general integer  $N$ , but we pick an odd prime  $p$

## Theorem (Shimura, 1958)

If

$$E : y^2 = 4x^3 - \frac{27Tx}{T-1728} - \frac{27T}{T-1728}$$

then  $\mathbf{Q}(T, E[p])$  is a finite Galois extension of  $\mathbf{Q}(T)$  with Galois group  $GL_2(\mathbf{Z}/p\mathbf{Z})$ . Moreover  $\mathbf{Q}(T, E[p]) \cap \overline{\mathbf{Q}} = \mathbf{Q}(\zeta_p)$  and  $\gamma \in GL_2(\mathbf{Z}/p\mathbf{Z})$  acts by  $\zeta_p \mapsto \zeta_p^{\det(\gamma)}$  so  $\mathbf{Q}(T, E[p])/\mathbf{Q}(T, \zeta_p)$  is a regular Galois extension with Galois group  $SL_2(\mathbf{Z}/p\mathbf{Z})$ .



# Proof of Shimura's Theorem I

To prove this, we work first over  $\mathbf{C}$  and consider the modular curves  $X(1), X(p)$ . We identify  $X(1)$  with  $\mathbb{P}^1$  and thus  $\mathbf{C}(X(1))$  with  $\mathbf{C}(T)$  using the above elliptic curve. We can show that  $\text{Gal}(\mathbf{C}(X(p))/\mathbf{C}(T)) = \text{PSL}_2(\mathbf{Z}/p\mathbf{Z})$  by considering the action of  $SL_2(\mathbf{Z})$  on  $\mathbf{C}(X(p))$  by  $(\gamma, f) \mapsto f \circ \gamma$ . The kernel of this action is  $\pm\Gamma(p)$  and the fixed field of this action is  $\mathbf{C}(X(1)) = \mathbf{C}(T)$ , so we have a Galois extension with Galois Group  $\text{PSL}_2(\mathbf{Z}/p\mathbf{Z})$ .

Then, following Diamond and Shurman, we can show that the trivial subgroup fixes the subextension generated by  $T$  and

$$f^{m,n}(\tau) = \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau \left( \frac{m\tau + n}{p} \right).$$

So we can identify  $\mathbf{C}(X(p))$  with  $\mathbf{C}(T, x(E[p]))$  since these functions are the  $x$  coordinates of the nontrivial  $p$ -torsion points of  $E$ .

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Repre-  
sentations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography



# Proof of Shimura's Theorem II

Certainly then  $\mathbf{C}(T, E[p])$  is a quadratic extension of  $\mathbf{C}(X(p))$  and with some work [D-S, Cor.7.5.3], one can prove that  $\text{Gal}(\mathbf{C}(T, E[p])/\mathbf{C}(T)) = \text{SL}_2(\mathbf{Z}/p\mathbf{Z})$ . To transfer this to  $\mathbf{Q}$ , we use the following:

## Theorem (The Weil Pairing)

*If  $E/k$  is an elliptic curve and  $n$  is an integer coprime to the characteristic of  $k$  then there is a canonical isomorphism of  $\text{Gal}(\bar{k}/k)$  modules  $e_n : \bigwedge^2 E[n] \xrightarrow{\sim} \mu_n$ .*

Moreover, the action of a Galois automorphism  $\sigma$  on  $E[n]$  taking the form of a matrix  $\gamma$  tells us that

$$\begin{aligned}\zeta_n^{\chi_{\text{cyc}}(\sigma)} &= \sigma(\zeta_n) = \sigma(e_n(P, Q)) = e_n(\sigma(P), \sigma(Q)) \\ &= e_n(\gamma(P, Q)) = e_n(P, Q)^{\det(\gamma)} = \zeta_n^{\det(\gamma)}\end{aligned}$$

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography



# Proof of Shimura's Theorem III

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Repre-  
sentations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

Since  $\mathbf{Q}(T, E[p])$  is generated over  $\mathbf{Q}(T)$  by the same equations that define  $\mathbf{C}(T, E[p])/\mathbf{C}(T)$ ,  $\mathbf{Q}(T, E[p])$  is a finite Galois extension. A restriction lemma [D-S, Lemma 7.6.2] shows that  $SL_2(\mathbf{Z}/p\mathbf{Z}) = Gal(\mathbf{Q}(T, E[p]) / (\mathbf{C}(T) \cap \mathbf{Q}(T, E[p])))$ , so  $\mathbf{Q}(T, \zeta_p) \supset (\mathbf{C}(T) \cap \mathbf{Q}(T, E[p]))$  while the other containment is trivial.

In particular,  $\mathbf{Q}(T, E[p]) \cap \overline{\mathbf{Q}} = \mathbf{Q}(\zeta_p)$ ,  
 $Gal(\mathbf{Q}(T, E[p]) / \mathbf{Q}(T, \zeta_p)) \cong SL_2(\mathbf{Z}/p\mathbf{Z})$  and since we earlier saw the determinant as the cyclotomic character,  
 $Gal(\mathbf{Q}(T, E[p]) / \mathbf{Q}(T)) \cong GL_2(\mathbf{Z}/p\mathbf{Z})$ .

As a Corollary, the homomorphisms  $\rho : G_{\mathbf{Q}(T)} \rightarrow GL_2(\mathbf{Z}/p\mathbf{Z})$   
and  $G_{\mathbf{Q}(T, \zeta_p)} \rightarrow SL_2(\mathbf{Z}/p\mathbf{Z})$  are onto.



# Overview

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

To prove Shih's theorem on Galois groups, we will:

- Use Shimura's result to construct new a Galois representation which is only a quadratic extension away from giving a regular field extension
- Introduce  $X_0(N)$  and how to obtain  $N$ -isogenies
- Construct a new representation using an  $N$  isogeny
- Show that in some cases this isogeny can make our quadratic ramification go away.
- Show that under further conditions, this representation is defined on  $G_{\mathbf{Q}(T)}$
- Use this new representation to give a regular Galois extension of  $\mathbf{Q}(T)$ , with the desired Galois Group.
- Use Hilbert's Irreducibility Theorem to get a Galois extension of  $\mathbf{Q}$ .



Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Repre-  
sentations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

We obtain a projective representation  $\bar{\rho}$  by composing  $\rho$  with the quotient map  $GL_2 \rightarrow PGL_2$ . As shown before, the determinant of  $\rho$  is the cyclotomic character so the kernel of  $\det \circ \rho$  defines  $\mathbf{Q}(T, \zeta_p)$  by the Galois correspondence. The kernel of  $\det \circ \bar{\rho}$  contains  $\ker(\det \circ \rho)$ . The image of  $\det \circ \bar{\rho}$  lies in  $(\mathbf{Z}/p\mathbf{Z})^\times / (\mathbf{Z}/p\mathbf{Z})^{\times 2}$ , so  $\ker(\det \circ \bar{\rho})$  has index two in  $G_{\mathbf{Q}(T)}$ .

An index two subgroup of  $G_{\mathbf{Q}(T)}$  gives a degree 2 extension  $K$  of  $\mathbf{Q}(T)$ , and since  $\ker(\det \circ \bar{\rho}) \supset \ker(\det \circ \rho)$ ,  $K \subset \mathbf{Q}(T, \zeta_p)$ . There is a unique quadratic subfield of a cyclotomic field, so  $K = \mathbf{Q}(T, \sqrt{p^*})$  where  $p^* = (-1)^{\frac{p-1}{2}} p$ .



# $X_0(N)$

The curve  $X_0(N)$  is a moduli space for the problem of classifying isogenies  $\phi : E_1 \rightarrow E_2$  where  $\ker(\phi) \cong \mathbf{Z}/N\mathbf{Z}$  or equivalently for pairs  $(E, C)$  where  $E$  is an elliptic curve and  $C$  is a subgroup of  $E$  isomorphic to  $\mathbf{Z}/N\mathbf{Z}$ . It admits a natural involution  $w_N$  such that  $w_N(\phi : E_1 \rightarrow E_2) = \widehat{\phi} : E_2 \rightarrow E_1$ .

$\mathbf{Q}(X_0(N))$  admits a description as  $\mathbf{Q}[T, S]/(F_N(T, S))$  where  $F_N$  is the Kronecker-Weber modular relation

$F_N(j(\tau), j(N\tau)) = 0$ . The effect of  $w_N$  on  $\mathbf{Q}(X_0(N))$  is to switch  $T$  with  $S$ .

We can also consider  $X_0^+(N) := X_0(N)/w_N$  so  $\mathbf{Q}(X_0(N))$  is a quadratic extension of  $\mathbf{Q}(X_0^+(N))$ . If we were to base extend  $E$  from  $\mathbf{Q}(X(1))$  to  $\mathbf{Q}(X_0(N))$  then we could let  $w_N$  act on  $E$  to obtain the Galois conjugate elliptic curve:

$$E^{w_N} : y^2 = 4x^3 - \frac{27Sx}{S - 1728} - \frac{27S}{S - 1728}$$

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Repre-  
sentations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography



# Galois Conjugate curves

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

## Definition ([Gross])

A  $K$ -curve is an elliptic curve which is defined over a finite field extension of  $K$  and is isogenous to its  $G_K$  Conjugates.

The Galois Conjugate  $E^{w_N}$  is  $N$ -isogenous to  $E$  so it is a  $\mathbf{Q}(X_0^+(N))$ -curve. We will shortly see the general fact that this allows us to extend the domain of the  $p$ -torsion representation. We have natural containments  $\mathbf{Q}(T) \subset \mathbf{Q}(X_0(N)) \subset \mathbf{Q}(X(N))$ , and if  $N, M$  are coprime then  $\mathbf{Q}(X(N)), \mathbf{Q}(X(M))$  are linearly disjoint over  $\mathbf{Q}(T) = \mathbf{Q}(X(1))$ . Hence the projective  $p$ -torsion representation of  $E$  is again surjective considered over  $\mathbf{Q}(X_0(N))$  if  $p \nmid N$ .

Let us now explicitly show how to extend the projective  $p$ -torsion representation of a  $K$ -curve  $E$  defined over a quadratic extension  $L$ .



# $K$ -curves and Galois Representations

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Repre-  
sentations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

If  $L/K$  is a quadratic extension with Galois group generated by  $\sigma$  and  $E$  is an elliptic curve without CM defined over  $L$  then suppose  $E$  is a  $K$ -curve, i.e. there is an isogeny  $\phi : E^\sigma \rightarrow E$ , which we can without loss of generality assume is cyclic. Let  $N = \# \ker \phi$ . If  $p \nmid N$  then  $\phi$  induces an isomorphism  $E^\sigma[p] \rightarrow E[p]$ . Since  $E$  (and thus  $E^\sigma$ ) does not have CM, the only automorphisms of  $E$  (and thus  $E^\sigma$ ) as elliptic curves are  $\pm 1$ . Thus the only  $N$ -isogenies are  $\pm \phi$  and so there is a unique isomorphism  $\mathbb{P}E^\sigma[p] \rightarrow \mathbb{P}E[p]$  induced by an  $N$ -isogeny. If  $s \in G_K - G_L$  then  $s$  sends  $E$  to  $E^\sigma$ . Thus  $\phi \circ s : E \rightarrow E^\sigma \rightarrow E$  and given a choice of basis for  $E[p]$  we define a representation  $G_K \rightarrow PGL_2(\mathbf{Z}/p\mathbf{Z})$  by the following action on  $\mathbb{P}E[p]$ :

$$\rho_{E,N}(s) := \begin{cases} s & s \in G_L \\ \phi \circ s & s \in G_K - G_L \end{cases}.$$



# $\rho_{E,N}$ is a homomorphism

Let  $s, t \in G_K$ . Then if  $s, t \in G_L$ ,  
 $\rho_{E,N}(st) = \bar{\rho}(st) = \bar{\rho}(s)\bar{\rho}(t) = \rho_{E,N}(s)\rho_{E,N}(t)$ . If  $t \in G_L$ ,  
 $s \in G_K - G_L$ , we drop the notation of  $\rho$  and simply say  
 $\rho_{E,N}(st) = \phi st = \rho_{E,N}(s)\rho_{E,N}(t)$ . If  $s \in G_L$ ,  $t \in G_K - G_L$ , we  
use the fact that the action of  $\phi$  on  $\mathbb{P}E[\rho]$  has to be  
 $G_L$ -equivariant (since  $\phi$  and  $s \circ \phi \circ s^{-1}$  are  $N$ -isogenies). Thus  
 $\rho_{E,N}(st) = \phi st = s\phi t = \rho_{E,N}(s)\rho_{E,N}(t)$ .  
Finally if  $s, t \in G_K - G_L$ ,  $\rho_{E,N}(s)\rho_{E,N}(t) = \phi s\{\phi\}t$ . One of  
the  $\phi$ 's is braced because we act on it by  $s^{-1}t \in G_L$ , giving  
 $\phi t\phi t^{-1}st$ . Now since  $t \in G_K - G_L$ ,  
 $t\phi t^{-1} : E \rightarrow E^\sigma \rightarrow E \rightarrow E^\sigma$ . Again, the only  $N$ -isogenies  
 $E \rightarrow E^\sigma$  are  $\pm\hat{\phi}$  so the action of the projectivization is uniquely  
 $\phi^{-1}$ , proving the proposition.

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography



# The character relation

Now suppose that  $K$  does not contain a square root of  $p^*$  and let  $\chi_p$  denote the quadratic character defining  $K(\sqrt{p^*})$ . Likewise let  $\chi_L$  denote the quadratic character defining  $L$ . As we saw before, using the Weil Pairing we can show  $\chi_p = \left(\frac{\det \circ \rho}{p}\right)$  where  $\rho$  is the non-projective  $p$ -torsion representation on  $E$ . We can relate these to the determinant character as follows:

## Theorem

$$\det \circ \rho_{E,N}(s) = \begin{cases} \chi_p & \left(\frac{N}{p}\right) = 1 \\ \chi_L \chi_p & \left(\frac{N}{p}\right) = -1 \end{cases}$$

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography



# Proof of the Character relation

First suppose that  $s|_L = 1$ . Up to the isomorphism  $(\mathbf{Z}/p\mathbf{Z})^\times / (\mathbf{Z}/p\mathbf{Z})^{\times 2} \cong \{\pm 1\}$  (which is just equality if  $p \equiv 3 \pmod{4}$ ), so

$$\det(\rho_{E,N}(s)) = \det(\bar{\rho}(s)) = \left( \frac{\det \circ \rho(s)}{p} \right) = \chi_p(s) = 1.$$

Now suppose  $s|_L = \sigma$  so  $\rho_{E,N}(s)$  is the matrix given by  $\phi \circ s$ . By definition  $\hat{\phi}\phi = [N]$ . To find a determinant we need only the effect on  $\mu_p = \bigwedge^2 E[p] = \bigwedge^2 E^\sigma[p]$ . If  $P, Q \in E[p]$  then

$$e_p(\phi sP, \phi sQ) = e_p(sP, \hat{\phi}\phi sQ) = e_p(sP, sQ)^N = e_p(P, Q)^{N\chi_{\text{cyc}}(s)}$$

Thus  $\det(\rho_{E,N}(s)) = \left(\frac{N}{p}\right) \chi_p(s)$ . If  $\left(\frac{N}{p}\right) = 1$  then regardless of  $s$ ,  $\det \rho_{E,N} = \chi_p$ . If  $\left(\frac{N}{p}\right) = -1$  then  $\det \rho_{E,N} = \pm \chi_p$  depending on whether  $s$  is in  $G_L$ , that is,  $\det \rho_{E,N} = \chi_L \chi_p$ .

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

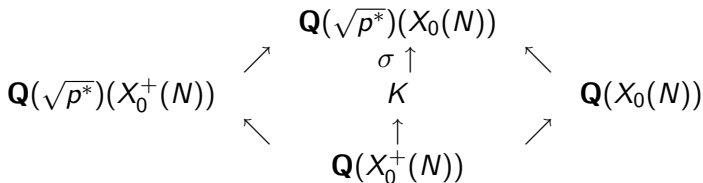
Finding  
rational points

Bibliography



# Twisting $X_0(N)$

Now since we have base extended  $E$  from  $\mathbf{Q}(X(1))$  to  $\mathbf{Q}(X_0(N))$ , we see that the  $p$ -torsion Galois representation extends to  $G_{\mathbf{Q}(X_0^+(N))}$ , but we have the same problem, that it defines a field extension which is still  $\sqrt{p^*}$  away from regularity. Thus consider the curve over  $\mathbf{Q}(\sqrt{p^*})(X_0(N))$ . The quadratic subfields give the diagram:





# Twisting $X_0(N)$

We can recognize  $K$  as follows. By Kummer theory  $\mathbf{Q}(X_0(N)) = \mathbf{Q}(X_0^+(N))(\sqrt{b})$  for some rational function  $b$  on  $X_0^+(N)$  so  $\mathbf{Q}(\sqrt{p^*})(X_0(N)) = \mathbf{Q}(X_0^+(N))(\sqrt{p^*}, \sqrt{b})$ . Thus  $K$  is the field  $\mathbf{Q}(X_0^+(N))(\sqrt{(p^*)b})$ . Alternately we can describe  $K$  as the function field over  $\mathbf{Q}$  for the curve  $C(N, p)$  given by twisting  $X_0(N)$  by  $w_N$  and  $\tau$ , the generator for  $\mathbf{Q}(\sqrt{p^*})/\mathbf{Q}$ . Thus  $\text{Gal}(\mathbf{Q}(\sqrt{p^*})(X_0(N))/\mathbf{Q}(C(N, p))) = \langle \sigma = w_N \tau \rangle$ . Since  $E$  is defined over  $\mathbf{Q}(T)$ ,  $E^\sigma = E^{w_N \tau} = E^{w_N}$  it fits the definition of a  $\mathbf{Q}(C(N, p))$ -curve. If  $L = \mathbf{Q}(\sqrt{p^*})(X_0(N)) = \mathbf{Q}(C(N, p))(\sqrt{p^*}) = K(\sqrt{p^*})$  we have  $\chi_L = \chi_p$  so  $\det \rho_{E, N} = \chi_p^2 = 1$  if  $\left(\frac{N}{p}\right) = -1$ . Suppose this is true, then  $\rho_{E, N}$  defines a Galois field extension  $M/\mathbf{Q}(C(N, p))$  such that  $M \cap \overline{\mathbf{Q}} \subset \mathbf{Q}(\sqrt{p^*})$ , but the action on  $\sqrt{p^*}$  is given by the determinant, which is now constantly 1. Hence  $\sqrt{p^*} \notin M$ , which we now see is a regular extension.

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Repre-  
sentations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography



$$\Lambda(N, p) \xrightarrow{PSL_2(\mathbf{Z}/p\mathbf{Z})} C(N, p)$$

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

Now by the curves/function field correspondence,  $M$  corresponds to a regular curve  $\Lambda(N, p)/C(N, p)$  whose group of automorphisms over  $C(N, p)$  is  $PSL_2(\mathbf{Z}/p\mathbf{Z})$ . In his paper, Serre proposed a complement which shows that if  $C(N, p)$  is a curve with infinitely many rational points, we can find a Galois extension of  $\mathbf{Q}$  with the same Galois group. The case that  $C(N, p)$  is a positive-rank elliptic curve has been dealt with by Clark [Clark]. We concern ourselves with determining when  $C(N, p) = \mathbb{P}^1$ , so  $\mathbf{Q}(C(N, p)) = \mathbf{Q}(T)$  and we can apply the classical version of Hilbert's Irreducibility Theorem.



# When is $C \cong \mathbb{P}^1$ ?

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

Recall the following criterion that a curve  $C$  is isomorphic to  $\mathbb{P}^1$ :

- $C$  has genus 0
- $C$  has a rational point

Since the genus is a geometric property and  $C(N, p) \cong X_0(N)$  after tensoring with  $\mathbf{Q}(\sqrt{p^*})$ , we recall the following:

## Lemma

*The genus of  $X_0(N)$  is zero for  $N = 1, 2, 3, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18$  or 25.*

This proof is simply computation from the genus formula for  $X_0(N)$  given in [D-S, §3.9].



# Using CM to find a point of $C(N, p)(\mathbf{Q})$

Now for the question of rational points, we make the following theorem:

## Theorem

*For  $N = 2, 3, 7$ , the fixed points of  $w_N$  are  $\mathbf{Q}$ -rational.*

## Part 1.

Consider  $\mathcal{O} = \mathbf{Z}[\sqrt{-N}]$  and the pair  $(E, E[\sqrt{-N}])$  where  $E$  has  $j$ -invariant  $j(\sqrt{-N})$ . Note that we have  $\widehat{\sqrt{-N}} = -\sqrt{-N}$  by definition and thus  $\#E[\sqrt{-N}] = \#E[-\sqrt{-N}] = N$  so this is indeed an element of  $X_0(N)$ . Moreover since  $\mathbf{Z}[\sqrt{-N}]$  has class number 1 in each case,  $E$  has rational (indeed integral by CM)  $j$ -invariant and can thus be defined over  $\mathbf{Q}$ . □

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography



# Using CM to find a point of $C(N, p)(\mathbf{Q})$

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Representations and  
Modular Curves

Galois Conjugates  
A new representation  
Twisting  $X_0(N)$

Finding rational points

Bibliography

## Part 2.

To see that  $E[\sqrt{-N}]$  is a rational subgroup we first consider that it is certainly  $G_{\mathbf{Q}(\sqrt{-N})}$ -invariant (since that group fixes  $\sqrt{-N}$ ). Thus we only need to see that if  $\sqrt{-N}(P) = O$  then  $\sqrt{-N}(\bar{P}) = O$ . Consider again the action of Galois on isogenies  $\phi \mapsto s\phi s^{-1}$  so  $s(\phi(P)) = s\phi(sP)$ . In our case

$$O = \bar{O} = \overline{\sqrt{-N}(P)} = \overline{\sqrt{-N}(\bar{P})} = -\sqrt{-N}(\bar{P}).$$

Thus  $O = -\sqrt{-N}(\bar{P})$  so  $\sqrt{-N}(\bar{P}) = O$  and  $E[\sqrt{-N}]$  is a  $\mathbf{Q}$ -rational cyclic order  $N$  subgroup. □



# Using CM to find a point of $C(N, p)(\mathbf{Q})$

## Part III.

Finally we show that our pair  $(E, E[\sqrt{-N}])$  is a fixed point of  $w_N$ . Since  $E[\sqrt{-N}]$  is by definition the kernel of  $\sqrt{-N} : E \rightarrow E$ , this must be the isogeny corresponding to our rational pair. The dual isogeny to  $\sqrt{-N}$  is  $-\sqrt{-N} : E \rightarrow E$  corresponding to  $(E, E[-\sqrt{-N}])$ . Then we can easily induce an isomorphism of pairs by the map  $[-1] : E \rightarrow E$ . □

Thus if  $N = 2, 3$  or  $7$ ,  $C(N, p) \cong \mathbb{P}^1$ , and we have the geometric portion of Shih's Theorem, that we have the curve  $\Lambda(N, p) \xrightarrow{PSL_2(\mathbf{Z}/p\mathbf{Z})} \mathbb{P}^1$ . By the curves/ function fields correspondence, we have a regular Galois field extension  $M_T \xrightarrow{PSL_2(\mathbf{Z}/p\mathbf{Z})} \mathbf{Q}(T)$ , and by Hilbert's Irreducibility Theorem, there are infinitely many  $a \in \mathbf{Q}$  such that  $M_a/\mathbf{Q}$  with Galois group  $PSL_2(\mathbf{Z}/p\mathbf{Z})$ .

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz

Introduction

Galois Repre-  
sentations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography



# Bibliography

Serre's  
Account of  
Shih's  
Theorem

Jim  
Stankewicz







Introduction

Galois Representations and  
Modular  
Curves

Galois  
Conjugates  
A new  
representation  
Twisting  $X_0(N)$

Finding  
rational points

Bibliography

-  Clark, P.; "Galois Groups via Atkin-Lehner Twists.", Proc. Amer. Math. Soc. Volume 138 No. 4 2007
-  Diamond, F., Shurman, J.; "A First Course in Modular Forms.", 2005, Springer GTM 228
-  Gross, B.; "Arithmetic on Elliptic Curves with Complex Multiplication.", 1980, Springer LNM 776
-  Serre, J.P.; "Topics in Galois Theory.", 1992, Jones and Bartlett
-  Shih, K.-y.; "On the Construction of Galois Extensions of Function Fields and Number Fields.", Mathematische Annalen, **207** 99-120, 1974
-  Shimura, G.; "Correspondances modulaires et les fonctions  $\zeta$  de courbes algébriques." J. Math. Soc. Japan **10** 1-28, 1958