ℓ-adic representations and congruences for congruences of modular forms

Ajay Prajapati

Indian Institute of Science, Bangalore

December 12, 2023

Overview

Overview

1 Introduction

2 The possible images

Ramanujan Δ function

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$$

Ramanujan Δ function

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

and the associated Dirichlet series has the Euler product expansion

$$\sum_{n=1}^{\infty}\tau(n)n^{-s} = \prod_{n=1}^{\infty}\frac{1}{(1-\tau(p)p^{-s}+p^{11-2s})}$$

Ramanujan Δ function

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

and the associated Dirichlet series has the Euler product expansion

$$\sum_{n=1}^{\infty}\tau(n)n^{-s} = \prod_{n=1}^{\infty}\frac{1}{(1-\tau(p)p^{-s}+p^{11-2s})}$$

Ramanujan was the first to observe that, modulo certain powers of certain small primes, there are congruences which connect $\tau(n)$ with some of the $\sigma_\nu(n)$.

Ramanujan Δ function

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

and the associated Dirichlet series has the Euler product expansion

$$\sum_{n=1}^{\infty}\tau(n)n^{-s} = \prod_{n=1}^{\infty}\frac{1}{(1-\tau(p)p^{-s}+p^{11-2s})}$$

Ramanujan was the first to observe that, modulo certain powers of certain small primes, there are congruences which connect $\tau(n)$ with some of the $\sigma_\nu(n)$.

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}$$

Congruences

$$\tau(n) \equiv \sigma_{11}(n) \pmod{2^{11}} \quad \text{if} \quad n \equiv 1 \pmod 8$$
$$\tau(n) \equiv 1217\sigma_{11}(n) \pmod{2^{13}} \quad \text{if} \quad n \equiv 3 \pmod 8$$
$$\tau(n) \equiv 1537\sigma_{11}(n) \pmod{2^{12}} \quad \text{if} \quad n \equiv 5 \pmod 8$$
$$\tau(n) \equiv 705\sigma_{11}(n) \pmod{2^{14}} \quad \text{if} \quad n \equiv 7 \pmod 8$$

Congruences

$$\tau(n) \equiv \sigma_{11}(n) \pmod{2^{11}} \quad \text{if} \quad n \equiv 1 \pmod 8$$
$$\tau(n) \equiv 1217\sigma_{11}(n) \pmod{2^{13}} \quad \text{if} \quad n \equiv 3 \pmod 8$$
$$\tau(n) \equiv 1537\sigma_{11}(n) \pmod{2^{12}} \quad \text{if} \quad n \equiv 5 \pmod 8$$
$$\tau(n) \equiv 705\sigma_{11}(n) \pmod{2^{14}} \quad \text{if} \quad n \equiv 7 \pmod 8$$

$$\tau(n) \equiv n^{-610}\sigma_{1231}(n) \pmod{3^{6}} \quad \text{if} \quad n \equiv 1 \pmod 3$$
$$\tau(n) \equiv n^{-610}\sigma_{1231}(n) \pmod{3^{7}} \quad \text{if} \quad n \equiv 2 \pmod 3$$

Congruences

$$\tau(n) \equiv \sigma_{11}(n) \pmod{2^{11}} \quad \text{if} \quad n \equiv 1 \pmod 8$$
$$\tau(n) \equiv 1217\sigma_{11}(n) \pmod{2^{13}} \quad \text{if} \quad n \equiv 3 \pmod 8$$
$$\tau(n) \equiv 1537\sigma_{11}(n) \pmod{2^{12}} \quad \text{if} \quad n \equiv 5 \pmod 8$$
$$\tau(n) \equiv 705\sigma_{11}(n) \pmod{2^{14}} \quad \text{if} \quad n \equiv 7 \pmod 8$$

$$\tau(n) \equiv n^{-610}\sigma_{1231}(n) \pmod{3^6} \quad \text{if} \quad n \equiv 1 \pmod 3$$
$$\tau(n) \equiv n^{-610}\sigma_{1231}(n) \pmod{3^7} \quad \text{if} \quad n \equiv 2 \pmod 3$$

$$\tau(n) \equiv n^{-30}\sigma_{71}(n) \pmod{5^3} \quad \text{if} \quad (n, 5) = 1$$

$$\tau(n) \equiv n\sigma_9(n) \pmod{7} \quad \text{if} \quad n \equiv 0, 1, 2, \text{ or } 4 \pmod{7}$$
$$\tau(n) \equiv n\sigma_9(n) \pmod{7^2} \quad \text{if} \quad n \equiv 3, 5, \text{ or } 7 \pmod{7}$$

$$\tau(n) \equiv n\sigma_9(n) \pmod 7 \quad \text{if} \quad n \equiv 0, 1, 2, \text{ or } 4 \pmod 7$$
$$\tau(n) \equiv n\sigma_9(n) \pmod{7^2} \quad \text{if} \quad n \equiv 3, 5, \text{ or } 7 \pmod 7$$

$$\tau(n) \equiv 0 \pmod{23} \quad \text{if} \quad \left(\frac{p}{23}\right) = 1$$
$$\tau(n) \equiv 2 \pmod{23} \quad \text{if} \quad p = u^2 + 23v^2 \text{ for integers } u \neq 0, v$$
$$\tau(n) \equiv -1 \pmod{23} \quad \text{for other } p \neq 23$$

$$\tau(n) \equiv n\sigma_9(n) \pmod 7 \quad \text{if} \quad n \equiv 0, 1, 2, \text{ or } 4 \pmod 7$$
$$\tau(n) \equiv n\sigma_9(n) \pmod{7^2} \quad \text{if} \quad n \equiv 3, 5, \text{ or } 7 \pmod 7$$

$$\tau(n) \equiv 0 \pmod{23} \quad \text{if} \quad \left(\frac{p}{23}\right) = 1$$
$$\tau(n) \equiv 2 \pmod{23} \quad \text{if} \quad p = u^2 + 23v^2 \text{ for integers } u \neq 0, v$$
$$\tau(n) \equiv -1 \pmod{23} \quad \text{for other } p \neq 23$$

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}$$

Two natural questions

1. Are there congruences for $\tau(n)$ modulo primes other than 2, 3, 5, 7, 23, and 691?

Two natural questions

1. Are there congruences for $\tau(n)$ modulo primes other than 2, 3, 5, 7, 23, and 691?
2. Are the congruences previously mentioned best possible or could one prove congruences modulo even higher powers?

Two natural questions

1. Are there congruences for $\tau(n)$ modulo primes other than 2, 3, 5, 7, 23, and 691?
2. Are the congruences previously mentioned best possible or could one prove congruences modulo even higher powers?
3. Are there similar congruences for fourier coefficients of other cusp forms?

Theorem (Serre-Deligne)

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, and suppose

Theorem (Serre-Deligne)

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, and suppose

1. $a_1 = 1$,

Theorem (Serre-Deligne)

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, and suppose

1. $a_1 = 1$,
2. every $a_n \in \mathbb{Z}$,

Theorem (Serre-Deligne)

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, and suppose

1. $a_1 = 1$,
2. every $a_n \in \mathbb{Z}$,
3. associated Dirichlet series has the Euler product expansion

$$\sum_{n=1}^{\infty} a_n n^{-s} = \prod_{n=1}^{\infty} \frac{1}{(1 - a_p p^{-s} + p^{11-2s})}$$

Theorem (Serre-Deligne)

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, and suppose

1. $a_1 = 1$,
2. every $a_n \in \mathbb{Z}$,
3. associated Dirichlet series has the Euler product expansion

$$\sum_{n=1}^{\infty} a_n n^{-s} = \prod_{n=1}^{\infty} \frac{1}{(1 - a_p p^{-s} + p^{11-2s})}$$

Then there is a continuous homomorphism

$$\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell),$$

depending on f,

Theorem (Serre-Deligne)

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$, and suppose

1. $a_1 = 1$,
2. every $a_n \in \mathbb{Z}$,
3. associated Dirichlet series has the Euler product expansion

$$\sum_{n=1}^{\infty} a_n n^{-s} = \prod_{n=1}^{\infty} \frac{1}{(1 - a_p p^{-s} + p^{11-2s})}$$

Then there is a continuous homomorphism

$$\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell),$$

depending on f, such that $\rho_\ell(\mathrm{Frob}_p)$ has char. polynomial

$$X^2 - a_p X + p^{k-1}$$

for each $p \neq \ell$.

1. Conditions on f are satisfied by unique cusp forms of weights 12, 16, 18, 20, 22, 26.

1. Conditions on f are satisfied by unique cusp forms of weights 12, 16, 18, 20, 22, 26.
2. This theorem implies

$$\det \circ\ \rho_\ell = \chi_\ell^{k-1}$$

1. Conditions on f are satisfied by unique cusp forms of weights 12, 16, 18, 20, 22, 26.
2. This theorem implies

$$\det \circ \ \rho_\ell = \chi_\ell^{k-1}$$

Intuition: If the image of ρ_ℓ is small enough, a knowledge of the determinant of an element of the image will imply some ℓ-adic information about the trace of that element;

1. Conditions on f are satisfied by unique cusp forms of weights 12, 16, 18, 20, 22, 26.
2. This theorem implies

$$\det \circ \ \rho_\ell = \chi_\ell^{k-1}$$

Intuition: If the image of ρ_ℓ is small enough, a knowledge of the determinant of an element of the image will imply some ℓ-adic information about the trace of that element; and so in particular a (approximate ℓ-adic) knowledge of p will imply some ℓ-adic information about a_p.

1. Conditions on f are satisfied by unique cusp forms of weights 12, 16, 18, 20, 22, 26.
2. This theorem implies

$$\det \circ \; \rho_\ell = \chi_\ell^{k-1}$$

   Intuition: If the image of ρ_ℓ is small enough, a knowledge of the determinant of an element of the image will imply some ℓ-adic information about the trace of that element; and so in particular a (approximate ℓ-adic) knowledge of p will imply some ℓ-adic information about a_p.
3. Converse also holds.

Lemma

Suppose that $\ell > 3$ and that $G \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup.

Lemma

Suppose that $\ell > 3$ and that $G \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup. If the image of G under the map

$$\pmod{\ell} : \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

contains $\mathrm{SL}_2(\mathbb{F}_\ell)$

Lemma

Suppose that $\ell > 3$ and that $G \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup. If the image of G under the map

$$(\bmod\ \ell) : \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ then G contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Proof (outline)

1. Let $G_n = \mathrm{Image}(G \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}))$.

Lemma

Suppose that $\ell > 3$ and that $G \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup. If the image of G under the map

$$(\bmod\ \ell) : \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ then G contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Proof (outline)

1. Let $G_n = \mathrm{Image}(G \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}))$. Enough to prove that $G_n \supset \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for each $n > 0$.

Lemma

Suppose that $\ell > 3$ and that $G \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup. If the image of G under the map

$$(\mathrm{mod}\ \ell) : \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ then G contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Proof (outline)

1. Let $G_n = \mathrm{Image}(G \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}))$. Enough to prove that $G_n \supset \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for each $n > 0$.
2. Let $H_n = \ker(\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z}))$.

Lemma

Suppose that $\ell > 3$ and that $G \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup. If the image of G under the map

$$(\bmod\ \ell) : \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ then G contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Proof (outline)

1. Let $G_n = \mathrm{Image}(G \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}))$. Enough to prove that $G_n \supset \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for each $n > 0$.
2. Let $H_n = \ker(\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z}))$. It is sufficient to prove that $H_n \subset G_n$ for each $n > 1$.

Lemma

Suppose that $\ell > 3$ and that $G \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup. If the image of G under the map

$$(\bmod\ \ell) : \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ then G contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Proof (outline)

1. Let $G_n = \mathrm{Image}(G \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}))$. Enough to prove that $G_n \supset \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for each $n > 0$.
2. Let $H_n = \ker(\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z}))$. It is sufficient to prove that $H_n \subset G_n$ for each $n > 1$.
3. H_2 is generated by three matrices $I + \ell u$ where $u = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$.

Proof Outline

1. In each case, $I + u \in \mathrm{SL}_2(\mathbb{Z})$ hence $\exists \sigma \in G$ such that $\sigma \equiv I + u \pmod{\ell}$.

Proof Outline

1. In each case, $I + u \in \mathrm{SL}_2(\mathbb{Z})$ hence $\exists \sigma \in G$ such that $\sigma \equiv I + u \pmod{\ell}$. i.e. $\sigma = I + u + \ell v$ where $v \in M_2(\mathbb{Z}_\ell)$.

Proof Outline

1. In each case, $I + u \in \mathrm{SL}_2(\mathbb{Z})$ hence $\exists \sigma \in G$ such that $\sigma \equiv I + u \pmod{\ell}$. i.e. $\sigma = I + u + \ell v$ where $v \in M_2(\mathbb{Z}_\ell)$. Now

$$\sigma^\ell = I + \ell(u + \ell v) + \ldots + (u + \ell v)^\ell \equiv I + \ell u \pmod{\ell^2}.$$

because $u^2 = 0$ in each case.

Proof Outline

1. In each case, $I + u \in \mathrm{SL}_2(\mathbb{Z})$ hence $\exists \sigma \in G$ such that $\sigma \equiv I + u \pmod{\ell}$. i.e. $\sigma = I + u + \ell v$ where $v \in M_2(\mathbb{Z}_\ell)$. Now

$$\sigma^\ell = I + \ell(u + \ell v) + \ldots + (u + \ell v)^\ell \equiv I + \ell u \pmod{\ell^2}.$$

because $u^2 = 0$ in each case.

2. So $G_2 \supset H_2$. Now we assume that $G_{n-1} \supset H_{n-1}$.

Proof Outline

1. In each case, $I + u \in \mathrm{SL}_2(\mathbb{Z})$ hence $\exists \sigma \in G$ such that $\sigma \equiv I + u \pmod{\ell}$. i.e. $\sigma = I + u + \ell v$ where $v \in M_2(\mathbb{Z}_\ell)$. Now
$$\sigma^\ell = I + \ell(u + \ell v) + \ldots + (u + \ell v)^\ell \equiv I + \ell u \pmod{\ell^2}.$$
because $u^2 = 0$ in each case.
2. So $G_2 \supset H_2$. Now we assume that $G_{n-1} \supset H_{n-1}$. Let $I + \ell^{n-1} v$ (with $v \in M_2(\mathbb{Z}_\ell)$) be representative of an element of G_n.
3. $I + \ell^{n-2} v \pmod{\ell^{n-1}}$ is in H_{n-1}.

Proof Outline

1. In each case, $I + u \in \mathrm{SL}_2(\mathbb{Z})$ hence $\exists \sigma \in G$ such that $\sigma \equiv I + u \pmod{\ell}$. i.e. $\sigma = I + u + \ell v$ where $v \in M_2(\mathbb{Z}_\ell)$. Now

$$\sigma^\ell = I + \ell(u + \ell v) + \ldots + (u + \ell v)^\ell \equiv I + \ell u \pmod{\ell^2}.$$

because $u^2 = 0$ in each case.

2. So $G_2 \supset H_2$. Now we assume that $G_{n-1} \supset H_{n-1}$. Let $I + \ell^{n-1} v$ (with $v \in M_2(\mathbb{Z}_\ell)$) be representative of an element of G_n.
3. $I + \ell^{n-2} v \pmod{\ell^{n-1}}$ is in H_{n-1}. By induction hypothesis, $\exists \sigma \in G$ such that

$$\sigma \equiv I + \ell^{n-2} v \pmod{\ell^{n-1}}.$$

Proof Outline

1. In each case, $I + u \in \mathrm{SL}_2(\mathbb{Z})$ hence $\exists \sigma \in G$ such that $\sigma \equiv I + u \pmod{\ell}$. i.e. $\sigma = I + u + \ell v$ where $v \in M_2(\mathbb{Z}_\ell)$. Now

$$\sigma^\ell = I + \ell(u + \ell v) + \ldots + (u + \ell v)^\ell \equiv I + \ell u \pmod{\ell^2}.$$

because $u^2 = 0$ in each case.

2. So $G_2 \supset H_2$. Now we assume that $G_{n-1} \supset H_{n-1}$. Let $I + \ell^{n-1} v$ (with $v \in M_2(\mathbb{Z}_\ell)$) be representative of an element of G_n.
3. $I + \ell^{n-2} v \pmod{\ell^{n-1}}$ is in H_{n-1}. By induction hypothesis, $\exists \sigma \in G$ such that

$$\sigma \equiv I + \ell^{n-2} v \pmod{\ell^{n-1}}.$$

Then

$$\sigma^\ell \equiv I + \ell^{n-1} v \pmod{\ell^n}.$$

Proof Outline

1. In each case, $I + u \in \mathrm{SL}_2(\mathbb{Z})$ hence $\exists \sigma \in G$ such that $\sigma \equiv I + u \pmod{\ell}$. i.e. $\sigma = I + u + \ell v$ where $v \in M_2(\mathbb{Z}_\ell)$. Now
$$\sigma^\ell = I + \ell(u + \ell v) + \ldots + (u + \ell v)^\ell \equiv I + \ell u \pmod{\ell^2}.$$
because $u^2 = 0$ in each case.
2. So $G_2 \supset H_2$. Now we assume that $G_{n-1} \supset H_{n-1}$. Let $I + \ell^{n-1} v$ (with $v \in M_2(\mathbb{Z}_\ell)$) be representative of an element of G_n.
3. $I + \ell^{n-2} v \pmod{\ell^{n-1}}$ is in H_{n-1}. By induction hypothesis, $\exists \sigma \in G$ such that
$$\sigma \equiv I + \ell^{n-2} v \pmod{\ell^{n-1}}.$$
Then
$$\sigma^\ell \equiv I + \ell^{n-1} v \pmod{\ell^n}.$$
So $G_n \supset H_n$.

There are analogous results for $\ell = 2$ and $\ell = 3$, in which $\mathbb{F}_\ell$ is replaced by $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$ respectively.

There are analogous results for $\ell = 2$ and $\ell = 3$, in which $\mathbb{F}_\ell$ is replaced by $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$ respectively.

Definition

ℓ is called an exceptional prime for the cusp form f if the image of ρ_ℓ does not contain $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

There are analogous results for $\ell = 2$ and $\ell = 3$, in which $\mathbb{F}_\ell$ is replaced by $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$ respectively.

Definition

ℓ is called an exceptional prime for the cusp form f if the image of ρ_ℓ does not contain $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Corollary

Suppose that $\ell > 3$; then ℓ is exceptional for $f \iff$ the image of $\widetilde{\rho}_\ell$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$.

There are analogous results for $\ell = 2$ and $\ell = 3$, in which $\mathbb{F}_\ell$ is replaced by $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$ respectively.

Definition

ℓ is called an exceptional prime for the cusp form f if the image of ρ_ℓ does not contain $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Corollary

Suppose that $\ell > 3$; then ℓ is exceptional for $f \iff$ the image of $\widetilde{\rho}_\ell$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$.
For $\ell = 2$ or 3 this is still a sufficient condition for ℓ to be exceptional for f.

Overview

Standard subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$

$\mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $V \cong \mathbb{F}_\ell^2$.

Standard subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$

$\mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $V \cong \mathbb{F}_\ell^2$.

Definition

A Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is any subgroup conjugate to the group of non-singular upper triangular matrices.

Standard subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$

$\mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $V \cong \mathbb{F}_\ell^2$.

Definition

A Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is any subgroup conjugate to the group of non-singular upper triangular matrices.

Definition

A Cartan subgroup is a maximal semi-simple commutative subgroup.

Standard subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$

$\mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $V \cong \mathbb{F}_\ell^2$.

Definition

A Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is any subgroup conjugate to the group of non-singular upper triangular matrices.

Definition

A Cartan subgroup is a maximal semi-simple commutative subgroup. For $\ell > 2$, a split Cartan subgroup is any subgroup conjugate to the group of non-singular diagonal matrices.

Standard subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$

$\mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $V \cong \mathbb{F}_\ell^2$.

Definition

A Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is any subgroup conjugate to the group of non-singular upper triangular matrices.

Definition

A Cartan subgroup is a maximal semi-simple commutative subgroup. For $\ell > 2$, a split Cartan subgroup is any subgroup conjugate to the group of non-singular diagonal matrices.

It is isomorphic to $(\mathbb{Z}/(\ell-1)\mathbb{Z})^2$.

Standard subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$

$\mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $V \cong \mathbb{F}_\ell^2$.

Definition

A Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is any subgroup conjugate to the group of non-singular upper triangular matrices.

Definition

A Cartan subgroup is a maximal semi-simple commutative subgroup. For $\ell > 2$, a split Cartan subgroup is any subgroup conjugate to the group of non-singular diagonal matrices.

It is isomorphic to $(\mathbb{Z}/(\ell-1)\mathbb{Z})^2$.
Similarly, non-split Cartan subgroup is defined. It is isomorphic to $\mathbb{F}_{\ell^2}^\times$.

Theorem

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Theorem

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.
If ℓ divides the order of G, then either

Theorem

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.
If ℓ divides the order of G, then either

1. G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, or

Theorem

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.
If ℓ divides the order of G, then either

1. G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, or
2. $\mathrm{GL}_2(\mathbb{F}_\ell) \subset G$.

Theorem

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.
If ℓ divides the order of G, then either

1. G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, or
2. $\mathrm{GL}_2(\mathbb{F}_\ell) \subset G$.

If $(|G|, \ell) = 1$, let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$; then

Theorem

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.
If ℓ divides the order of G, then either

1. G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, or
2. $\mathrm{GL}_2(\mathbb{F}_\ell) \subset G$.

If $(|G|, \ell) = 1$, let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$; then

1. H is cyclic and G is contained in a Cartan subgroup, or

Theorem

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.
If ℓ divides the order of G, then either

1. G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, or
2. $\mathrm{GL}_2(\mathbb{F}_\ell) \subset G$.

If $(|G|, \ell) = 1$, let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$; then

1. H is cyclic and G is contained in a Cartan subgroup, or
2. H is dihedral and G is contained in the normalizer of a Cartan subgroup but not in the Cartan subgroup itself, or

Theorem

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.
If ℓ divides the order of G, then either

1. G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, or
2. $\mathrm{GL}_2(\mathbb{F}_\ell) \subset G$.

If $(|G|, \ell) = 1$, let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$; then

1. H is cyclic and G is contained in a Cartan subgroup, or
2. H is dihedral and G is contained in the normalizer of a Cartan subgroup but not in the Cartan subgroup itself, or
3. H is isomorphic to A_4, S_4, or A_5.

In case (ii) ℓ must be odd;

Theorem

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.
If ℓ divides the order of G, then either

1. G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, or
2. $\mathrm{GL}_2(\mathbb{F}_\ell) \subset G$.

If $(|G|, \ell) = 1$, let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$; then

1. H is cyclic and G is contained in a Cartan subgroup, or
2. H is dihedral and G is contained in the normalizer of a Cartan subgroup but not in the Cartan subgroup itself, or
3. H is isomorphic to A_4, S_4, or A_5.

In case (ii) ℓ must be odd;
in case (iii) ℓ must be prime to 6, 6, or 30 respectively.

Corollary 1

Let $\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ be any continuous homomorphism such that

$$\det \circ \ \rho_\ell = \chi_\ell^{k-1}$$

for some even integer k.

Corollary 1

Let $\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ be any continuous homomorphism such that

$$\det \circ \ \rho_\ell = \chi_\ell^{k-1}$$

for some even integer k. Let $G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be the image of $\widetilde{\rho}_\ell$ and let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$.

Corollary 1

Let $\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ be any continuous homomorphism such that

$$\det \circ \ \rho_\ell = \chi_\ell^{k-1}$$

for some even integer k. Let $G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be the image of $\widetilde{\rho}_\ell$ and let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Suppose that G does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$.

Corollary 1

Let $\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ be any continuous homomorphism such that

$$\det \circ \ \rho_\ell = \chi_\ell^{k-1}$$

for some even integer k. Let $G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be the image of $\widetilde{\rho}_\ell$ and let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Suppose that G does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$. Then

1. G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$; or

Corollary 1

Let $\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ be any continuous homomorphism such that

$$\det \circ \ \rho_\ell = \chi_\ell^{k-1}$$

for some even integer k. Let $G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be the image of $\widetilde{\rho}_\ell$ and let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Suppose that G does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$. Then

1. G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$; or
2. G is contained in the normalizer of a Cartan subgroup, but not in the Cartan subgroup itself; or

Corollary 1

Let $\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ be any continuous homomorphism such that

$$\det \circ \ \rho_\ell = \chi_\ell^{k-1}$$

for some even integer k. Let $G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be the image of $\widetilde{\rho}_\ell$ and let H be the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Suppose that G does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$. Then

1. G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$; or
2. G is contained in the normalizer of a Cartan subgroup, but not in the Cartan subgroup itself; or
3. $H \cong S_4$.

Proof Outline

1. Any subgroup of a split Cartan subgroup is contained in a Borel subgroup.

Proof Outline

1. Any subgroup of a split Cartan subgroup is contained in a Borel subgroup.
2. Let C be a non-split Cartan subgroup. So C is cyclic of order $(\ell^2 - 1)$.

Proof Outline

1. Any subgroup of a split Cartan subgroup is contained in a Borel subgroup.
2. Let C be a non-split Cartan subgroup. So C is cyclic of order $(\ell^2 - 1)$. Now $\widetilde{\rho}_\ell$ factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$.
3. Since $(|Im(\mathbb{Z}_\ell^*)|, \ell) = 1$, $|Im(\mathbb{Z}_\ell^*)| \mid (\ell - 1)$.

Proof Outline

1. Any subgroup of a split Cartan subgroup is contained in a Borel subgroup.
2. Let C be a non-split Cartan subgroup. So C is cyclic of order $(\ell^2 - 1)$. Now $\widetilde{\rho}_\ell$ factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$.
3. Since $(|Im(\mathbb{Z}_\ell^*)|, \ell) = 1$, $|Im(\mathbb{Z}_\ell^*)| \mid (\ell - 1)$. Thus image lies in a Borel subgroup.
4. Now we prove that $H \neq A_4$ or A_5.

Proof Outline

1. Any subgroup of a split Cartan subgroup is contained in a Borel subgroup.
2. Let C be a non-split Cartan subgroup. So C is cyclic of order $(\ell^2 - 1)$. Now $\widetilde{\rho}_\ell$ factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$.
3. Since $(|Im(\mathbb{Z}_\ell^*)|, \ell) = 1$, $|Im(\mathbb{Z}_\ell^*)| \mid (\ell - 1)$. Thus image lies in a Borel subgroup.
4. Now we prove that $H \neq A_4$ or A_5. We assume $\ell > 2$. Consider the commutative diagram:

$$\begin{array}{ccccc} \mathrm{Gal}(K_\ell/\mathbb{Q}) & \longrightarrow & G & \xrightarrow{\quad det \quad} & \mathbb{F}_\ell^* \\ & & \downarrow & & \downarrow \\ & & H & \longrightarrow & \mathbb{F}_\ell^*/{\mathbb{F}_\ell^*}^2 \cong \{\pm 1\} \end{array}$$

Proof Outline

1. Any subgroup of a split Cartan subgroup is contained in a Borel subgroup.
2. Let C be a non-split Cartan subgroup. So C is cyclic of order $(\ell^2 - 1)$. Now $\widetilde{\rho}_\ell$ factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$.
3. Since $(|Im(\mathbb{Z}_\ell^*)|, \ell) = 1$, $|Im(\mathbb{Z}_\ell^*)| \mid (\ell - 1)$. Thus image lies in a Borel subgroup.
4. Now we prove that $H \neq A_4$ or A_5. We assume $\ell > 2$. Consider the commutative diagram:

$$\begin{array}{ccccc}
\mathrm{Gal}(K_\ell/\mathbb{Q}) & \longrightarrow & G & \xrightarrow{det} & \mathbb{F}_\ell^* \\
 & & \downarrow & & \downarrow \\
 & & H & \longrightarrow & \mathbb{F}_\ell^*/{\mathbb{F}_\ell^*}^2 \cong \{\pm 1\}
\end{array}$$

Image of G in $\mathbb{F}_\ell^*$ consists of all $(k-1)^{th}$ powers and k is even.

Corollary 2

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ be a normalized eigenform and ρ_ℓ be the Galois representation given by Serre-Deligne.

Corollary 2

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ be a normalized eigenform and ρ_ℓ be the Galois representation given by Serre-Deligne. Suppose that the image of $\widetilde{\rho_\ell}$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, so that ℓ is an exceptional prime for f.

Corollary 2

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ be a normalized eigenform and ρ_ℓ be the Galois representation given by Serre-Deligne. Suppose that the image of $\widetilde{\rho}_\ell$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, so that ℓ is an exceptional prime for f.

Then the three cases listed in Corollary 1 imply respectively the following congruences for the coefficients of f

Corollary 2

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ be a normalized eigenform and ρ_ℓ be the Galois representation given by Serre-Deligne. Suppose that the image of $\widetilde{\rho}_\ell$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, so that ℓ is an exceptional prime for f.
Then the three cases listed in Corollary 1 imply respectively the following congruences for the coefficients of f

1. There is an integer m such that

$$a_n \equiv n^m \sigma_{k-1-2m}(n) \pmod{\ell}$$

for all n prime to ℓ.

Corollary 2

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ be a normalized eigenform and ρ_ℓ be the Galois representation given by Serre-Deligne. Suppose that the image of $\widetilde{\rho}_\ell$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, so that ℓ is an exceptional prime for f.
Then the three cases listed in Corollary 1 imply respectively the following congruences for the coefficients of f

1. There is an integer m such that

$$a_n \equiv n^m \sigma_{k-1-2m}(n) \pmod{\ell}$$

   for all n prime to ℓ.

2. $a_n \equiv 0 \pmod{\ell}$ whenever n is a quadratic non-residue $(\mathrm{mod}\ \ell)$.

Corollary 2

Let $f = \Sigma a_n q^n \in \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ be a normalized eigenform and ρ_ℓ be the Galois representation given by Serre-Deligne. Suppose that the image of $\widetilde{\rho}_\ell$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, so that ℓ is an exceptional prime for f.
Then the three cases listed in Corollary 1 imply respectively the following congruences for the coefficients of f

1. There is an integer m such that
$$a_n \equiv n^m \sigma_{k-1-2m}(n) \pmod{\ell}$$
for all n prime to ℓ.
2. $a_n \equiv 0 \pmod{\ell}$ whenever n is a quadratic non-residue $\pmod{\ell}$.
3. $p^{1-k} a_p^2 \equiv 0,\ 1,\ 2,$ or $4 \pmod{\ell}$ for all primes $p \neq \ell$.

Proof Outline

1. WLOG, can assume that Borel consists of upper triangular matrices.

Proof Outline

1. WLOG, can assume that Borel consists of upper triangular matrices. Thus for any $\sigma \in \mathrm{Gal}(K_\ell/\mathbb{Q})$, we can write

$$\widetilde{\rho}_\ell = \begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & d(\sigma) \end{pmatrix}$$

Proof Outline

1. WLOG, can assume that Borel consists of upper triangular matrices. Thus for any $\sigma \in \mathrm{Gal}(K_\ell/\mathbb{Q})$, we can write

$$\widetilde{\rho}_\ell = \begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & d(\sigma) \end{pmatrix}$$

2. So $a(\sigma) : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathbb{F}_\ell^*$ is a continuous homomorphism

Proof Outline

1. WLOG, can assume that Borel consists of upper triangular matrices. Thus for any $\sigma \in \mathrm{Gal}(K_\ell/\mathbb{Q})$, we can write

$$\widetilde{\rho}_\ell = \begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & d(\sigma) \end{pmatrix}$$

2. So $a(\sigma) : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathbb{F}_\ell^*$ is a continuous homomorphism hence equals $\widetilde{\chi}_\ell{}^m$.

Proof Outline

1. WLOG, can assume that Borel consists of upper triangular matrices. Thus for any $\sigma \in \mathrm{Gal}(K_\ell/\mathbb{Q})$, we can write

$$\widetilde{\rho}_\ell = \begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & d(\sigma) \end{pmatrix}$$

2. So $a(\sigma) : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathbb{F}_\ell^*$ is a continuous homomorphism hence equals $\widetilde{\chi}_\ell{}^m$. So $d = \widetilde{\chi}_\ell{}^{k-1-m}$ and

Proof Outline

1. WLOG, can assume that Borel consists of upper triangular matrices. Thus for any $\sigma \in \mathrm{Gal}(K_\ell/\mathbb{Q})$, we can write
$$\widetilde{\rho}_\ell = \begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & d(\sigma) \end{pmatrix}$$
2. So $a(\sigma) : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathbb{F}_\ell^*$ is a continuous homomorphism hence equals ${\widetilde{\chi}_\ell}^m$. So $d = {\widetilde{\chi}_\ell}^{k-1-m}$ and
$$a_p \equiv p^m + p^{k-1-m} \pmod{\ell}$$
for $p \neq \ell$.
3. Let C be the Cartan subgroup and N its normalizer, and consider the homomorphism
$$\mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow N \longrightarrow N/C \cong \{\pm 1\}$$

Proof Outline

1. It factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$.

Proof Outline

1. It factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$. The only continuous homomorphism of $\mathbb{Z}_\ell^*$ onto $\{\pm 1\}$ is $x \longmapsto x^2$.

Proof Outline

1. It factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$. The only continuous homomorphism of $\mathbb{Z}_\ell^*$ onto $\{\pm 1\}$ is $x \longmapsto x^2$.
2. $\widetilde{\rho}_\ell(\mathrm{Frob}(p))$ is in $C \iff p$ is a quadratic residue $\pmod{\ell}$.

Proof Outline

1. It factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$. The only continuous homomorphism of $\mathbb{Z}_\ell^*$ onto $\{\pm 1\}$ is $x \longmapsto x^2$.
2. $\widetilde{\rho}_\ell(\mathrm{Frob}(p))$ is in $C \iff p$ is a quadratic residue $\pmod{\ell}$.
3. Let $\alpha \in N - C$. Then it interchanges the two one-dimensional subspaces on which it operates.

Proof Outline

1. It factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$. The only continuous homomorphism of $\mathbb{Z}_\ell^*$ onto $\{\pm 1\}$ is $x \longmapsto x^2$.
2. $\widetilde{\rho}_\ell(\mathrm{Frob}(p))$ is in $C \iff p$ is a quadratic residue $\pmod{\ell}$.
3. Let $\alpha \in N - C$. Then it interchanges the two one-dimensional subspaces on which it operates. So can be put in the form $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$. So $\mathrm{Trace}(\alpha) = 0$.

Proof Outline

1. It factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$. The only continuous homomorphism of $\mathbb{Z}_\ell^*$ onto $\{\pm 1\}$ is $x \longmapsto x^2$.
2. $\widetilde{\rho}_\ell(\mathrm{Frob}(p))$ is in $C \iff p$ is a quadratic residue $\pmod{\ell}$.
3. Let $\alpha \in N - C$. Then it interchanges the two one-dimensional subspaces on which it operates. So can be put in the form $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$. So $\mathrm{Trace}(\alpha) = 0$.
4. For (iii), use every element of H has order $1, 2, 3$ or 4.

Proof Outline

1. It factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$. The only continuous homomorphism of $\mathbb{Z}_\ell^*$ onto $\{\pm 1\}$ is $x \longmapsto x^2$.
2. $\widetilde{\rho}_\ell(\mathrm{Frob}(p))$ is in $C \iff p$ is a quadratic residue $\pmod{\ell}$.
3. Let $\alpha \in N - C$. Then it interchanges the two one-dimensional subspaces on which it operates. So can be put in the form $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$. So $\mathrm{Trace}(\alpha) = 0$.
4. For (iii), use every element of H has order $1, 2, 3$ or 4.
5. **We may distinguish (iii) from (ii) as follows:** By an argument similar to used for (ii), the image of $\mathrm{Frob}(p) \in A_4 \iff p$ is a quadratic residue $\pmod{\ell}$.

Proof Outline

1. It factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$. The only continuous homomorphism of $\mathbb{Z}_\ell^*$ onto $\{\pm 1\}$ is $x \longmapsto x^2$.
2. $\widetilde{\rho}_\ell(\mathrm{Frob}(p))$ is in $C \iff p$ is a quadratic residue $\pmod{\ell}$.
3. Let $\alpha \in N - C$. Then it interchanges the two one-dimensional subspaces on which it operates. So can be put in the form $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$. So $\mathrm{Trace}(\alpha) = 0$.
4. For (iii), use every element of H has order $1, 2, 3$ or 4.
5. **We may distinguish (iii) from (ii) as follows:** By an argument similar to used for (ii), the image of $\mathrm{Frob}(p) \in A_4 \iff p$ is a quadratic residue $\pmod{\ell}$.
6. There are infinitely many p such that $\mathrm{Frob}(p)$ has order 4.

Proof Outline

1. It factors through $\mathrm{Gal}(K_\ell^{ab}/\mathbb{Q}) \cong \mathbb{Z}_\ell^*$. The only continuous homomorphism of $\mathbb{Z}_\ell^*$ onto $\{\pm 1\}$ is $x \longmapsto x^2$.
2. $\widetilde{\rho}_\ell(\mathrm{Frob}(p))$ is in $C \iff p$ is a quadratic residue $\pmod{\ell}$.
3. Let $\alpha \in N - C$. Then it interchanges the two one-dimensional subspaces on which it operates. So can be put in the form $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$. So $\mathrm{Trace}(\alpha) = 0$.
4. For (iii), use every element of H has order $1, 2, 3$ or 4.
5. **We may distinguish (iii) from (ii) as follows:** By an argument similar to used for (ii), the image of $\mathrm{Frob}(p) \in A_4 \iff p$ is a quadratic residue $\pmod{\ell}$.
6. There are infinitely many p such that $\mathrm{Frob}(p)$ has order 4. For such p's, $p^{1-k}a_p^2 \equiv 2 \pmod{\ell}$.