Numerical study of Serre's modularity conjecture over imaginary quadratic fields with Magma

Shun'ichi Yokoyama (Kyushu University)

March 18, 2010 / KANT 2010

Today's outline

- Brief introduction to Serre's modularity conjecture over imaginary quadratic fields
  - Bianchi modular forms
  - Galois representations over imaginary quadratic fields
- Computational Approach (with Magma)
  - Cohomology computation
  - Searching number fields with prescribed ramification using (Targeted) Martinet Search

Serre's modularity conjecture

- Relation between Galois representations and modular forms.
- Proved by Khare and Wintenberger.
  (over $\mathbb{Q}$, 2007)

Theorem (Khare-Wintenberger, 2007)

Any odd, irreducible Galois representation over $\mathbb{Q}$

$$\rho : \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

arises from a cusp form of type $(N(\rho), k(\rho), \epsilon(\rho))$

$$f = \sum_{n \geq 1} a_n q^n \quad \left(q = e^{2\pi i z}\right) \ \in S_{k(\rho)}(\Gamma, \epsilon(\rho)) \ .$$

i.e. $\mathrm{Tr}(\rho(\mathrm{Frob}_l)) \equiv a_l \pmod{p}$ *for all* $l \nmid pN(\rho)$*: prime*

Serre's modularity conjecture

Generalized conjecture (GL(2)-case)

	base field	associated to
A	rat'l (odd)	weight 2 cusp form over $\mathbb{Q}$
B	rat'l (even)	Maass wave form
C	totally real	Hilbert modular form
D	**imaginary quad.**	**Bianchi modular form** (cohomological)

Preceding studies:

- Cremona(1980s): hyperbolic tessellation / modular symbols
- Figueiredo(1990s): homological approach $\to$ computational approach
    - Torrey(2009): homological approach
    - Şengün(2008, 2009): cohomological approach

Main Results

K: imaginary quadratic field

- Hecke Side : Bianchi modular form $H^1(\Gamma, E_k(\overline{\mathbb{F}}_p))$
  - Computing the space of eigenvalue system of small level and weight.
- Galois Side : $\rho_K : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$
  - (Restrict ramification) Searching number fields L which satisfy $\mathrm{Gal}(L/\mathbb{Q}) \simeq A_4$,
    Construct $\rho_K : \mathrm{Gal}(L/K) \to \mathrm{SL}_2(\mathbb{F}_3)$ and compute $\mathrm{Tr}(\rho_K(\mathrm{Frob}_{\mathcal{P}}))$.
  - (Restrict ramification) Searching number fields L which satisfy $\mathrm{Gal}(L/K) \simeq A_5$,
    ※ Compute $\rho_K : \mathrm{Gal}(L/K) \to \mathrm{SL}_2(\mathbb{F}_4)$:Now in progress.
- Comparison

Hecke Side - Bianchi modular forms

Definition

A Bianchi modular form of level $\mathcal{I}$ and weight (k_1, k_2) is a cohomology class in $H^1(\Gamma_1(\mathcal{I}), E_{k_1,k_2}(\mathbb{C}))$.
It is cuspidal if it is in the cuspidal part $H^1_{cusp}(\Gamma_1(\mathcal{I}), E_{k_1,k_2}(\mathbb{C}))$.

- $\mathcal{I}$: ideal of $\mathcal{O}_K$.
- $\Gamma_1(\mathcal{I}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod \mathcal{I} \right\}$
- $E_k(\mathbb{C})$: Space of homogeneous polynomials of degree k in two variables with coefficients in $\mathbb{C}$.
- $E_{k_1,k_2}(\mathbb{C}) = E_{k_1}(\mathbb{C}) \otimes \overline{E}_{k_2}(\mathbb{C})$ $(\overline{E}$:complex conjugation$)$.

Hecke Side - Bianchi modular forms

Definition (mod p version)

A mod p Bianchi modular form of level $\mathcal{I}$ and weight (k_1, k_2) is a cohomology class in $H^1(\Gamma_1(\mathcal{I}), E_{k_1,k_2}(\overline{\mathbb{F}}_p))$.
It is cuspidal if it is in the cuspidal part $H^1_{cusp}(\Gamma_1(\mathcal{I}), E_{k_1,k_2}(\overline{\mathbb{F}}_p))$.

- $\mathcal{I}$: ideal of $\mathcal{O}_K$.
- $\Gamma_1(\mathcal{I}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod \mathcal{I} \right\}$
- $p = \lambda\overline{\lambda}$
- $E_k(\mathbb{F}_p)$: Space of homogeneous polynomials of degree k in two variables with coefficients in $\mathbb{F}_p$.
- $E_{k_1,k_2}(\mathbb{F}_p) = E_{k_1}(\mathbb{F}_p) \otimes \overline{E}_{k_2}(\mathbb{F}_p)$ ($\overline{E}$:mod $\overline{\lambda}$ reduction) .

Serre's conjecture over K

Conjecture

An absolutely irreducible mod p Galois representation $\rho_K : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ comes from some eigenform (mod p Bianchi cusp form).

i.e., there is a mod p Bianchi modular form $f \in H^1_{cusp}(\Gamma_1(\mathcal{I}), E(\overline{\mathbb{F}}_p))$ which is an eigenform for all Hecke operators s.t.

$$\mathrm{Tr}\left(\rho_K(\mathrm{Frob}_\lambda)\right) = a_\lambda \ , \ \det\left(\rho_K(\mathrm{Frob}_\lambda)\right) = b_\lambda N(\lambda) \ .$$

for all primes $\lambda \nmid p\mathcal{I}$ at which ρ is unramified. Here a_λ, b_λ are the eigenvalues of f under the Hecke operators T_λ, S_λ respectively:

$$T_\lambda f = a_\lambda f \ , \quad S_\lambda f = b_\lambda f \ .$$

Here $N(\lambda)$ is the norm of λ over $\mathbb{Q}$.

Flow chart

- Finite presentation of $\mathrm{PSL}_2(\mathcal{O}_K)$
  - Case of $K = \mathbb{Q}(\sqrt{-1})$:

$$\mathrm{PSL}_2(\mathcal{O}_K) = \left\langle A, B, U \;\middle|\; \begin{array}{l} B^2 = (AB)^3 = (BUBU^{-1})^3 = AUA^{-1}U^{-1} \\ = (BU^2BU^{-1})^2 = (AUBAU^{-1}B)^2 = 1 \end{array} \right\rangle$$

where $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $U = \begin{pmatrix} 1 & 0 \\ \sqrt{-1} & 1 \end{pmatrix}$.

  - Case of $K = \mathbb{Q}(\sqrt{-2})$:

$$\mathrm{PSL}_2(\mathcal{O}_K) = \langle A, B, U \mid B^2 = (AB)^3 = AUAU^{-1} = (BU^{-1}BU)^2 = 1 \rangle$$

where $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $U = \begin{pmatrix} 1 & 0 \\ \sqrt{-2} & 1 \end{pmatrix}$.

Flow chart

- Action of Hecke operator

$$(T_\pi c)(g) = \sum_j c(\alpha^{-1} h_j(g)\alpha)\alpha^\iota R_j^{-1}$$

where

- $c \in H^1(\Gamma, E_k)$,
- $g \in \Gamma$,
- $\alpha = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}$ where π is a prime of $\mathcal{O}_K$ s.t. $N(\pi) = p$,
- $\alpha^\iota = \det(\alpha)\alpha^{-1}$.

Flow chart

- $P_M(n) = \begin{cases} M^{n-1} + \cdots + M^2 + M + 1 & n > 0 , \\ -(M^{-n-1} + \cdots + M^2 + M + 1)M^n & n < 0 \end{cases}$

$$
\begin{aligned}
(T_\pi c)(A) &= c(A)\left[P_A(a)(U^{-b}B\alpha^\iota B + U^b\alpha^\iota)\right] \\
&\quad + c(B)\left[(A^a U^{-b}B + 1)(\alpha^\iota B)\right] \\
&\quad + c(U)\left[P_U(-b)B\alpha^\iota B + P_U(b)\alpha^\iota\right] , \\
(T_\pi c)(U) &= c(A)\left[\left(\sum_{0\le j\le p-1} P_A(\mathrm{Re}(j))U^{\mathrm{Im}(j)}B\alpha^\iota BA^j\right) + P_A(-2b)U^a\alpha^\iota\right] \\
&\quad + c(B)\left[\sum_{0\le j\le p-1}\left(A^{\mathrm{Re}(j)}U^{\mathrm{Im}(j)}B + 1\right)\left(\alpha^\iota BA^j\right)\right] \\
&\quad + c(U)\left[\left(\sum_{0\le j\le p-1} P_U(\mathrm{Im}(j))B\alpha^\iota BA^j\right) + P_U(a)\alpha^\iota\right]
\end{aligned}
$$

Flow chart

$$
\begin{aligned}
(T_\pi c)(B) &= \sum_{1 \le j \le p-1} c(\alpha^{-1} h_j(B)\alpha)\alpha^\iota R_j^{-1} \\
&= \sum_{1 \le j \le p-1} c\left(\begin{pmatrix} \sigma_B(j) & \frac{1+j\sigma_B(j)}{\pi} \\ -\pi & -j \end{pmatrix}\right)\alpha^\iota B A^j ,
\end{aligned}
$$

\+ word decomposition

$$M = \pm Q_m B Q_{m-1} \cdots B Q_2 B Q_1 \ \text{ or } \ M = \pm B Q_m B Q_{m-1} \cdots B Q_2 B Q_1$$

where $M \in \mathrm{PSL}_2(\mathcal{O}_K)$ and Q_i is lower triangular:

$$Q_i = A^a U^b$$

Result: Example

$K = \mathbb{Q}(\sqrt{-2}),\ T(\mathcal{P}) \curvearrowright H^1(\Gamma_0(\mathcal{I}), E_{1,1}(\mathbb{C})),\ N(\mathcal{I}) = 3,\ N(\mathcal{P}) < 100$

$\mathcal{P}$	eigenvalue
$1 \pm \sqrt{2}i$	-2
$3 \pm \sqrt{2}i$	14
$3 \pm 2\sqrt{2}i$	2
$1 \pm 3\sqrt{2}i$	-34
$3 \pm 4\sqrt{2}i$	-46
$5 \pm 3\sqrt{2}i$	14
$3 \pm 5\sqrt{2}i$	-82
$7 \pm 3\sqrt{2}i$	62
$1 \pm 6\sqrt{2}i$	-142
$9 \pm \sqrt{2}i$	158
$9 \pm 2\sqrt{2}i$	146
$5 \pm 6\sqrt{2}i$	-94

Result: Example

$$K = \mathbb{Q}(\sqrt{-2}),\ T(\mathcal{P}) \curvearrowright H^1(\Gamma_0(\mathcal{I}), E_{3,3}(\mathbb{C})),\ N(\mathcal{I}) = 3,\ N(\mathcal{P}) < 100$$

$\mathcal{P}$	eigenvalue	
$1 \pm \sqrt{2}i$	-14	6
$3 \pm \sqrt{2}i$	-46	-26
$3 \pm 2\sqrt{2}i$	-574	226
$1 \pm 3\sqrt{2}i$	434	134
$3 \pm 4\sqrt{2}i$	-1246	994
$5 \pm 3\sqrt{2}i$	-3502	-1882
$3 \pm 5\sqrt{2}i$	-238	-5018
$7 \pm 3\sqrt{2}i$	-5134	8006
$1 \pm 6\sqrt{2}i$	9506	386
$9 \pm \sqrt{2}i$	11186	-2234
$9 \pm 2\sqrt{2}i$	5474	-10046
$5 \pm 6\sqrt{2}i$	-9982	8738

Result: Example

$$K = \mathbb{Q}(\sqrt{-1}),\ T(\mathcal{P}) \curvearrowright H^1(\Gamma_0(\mathcal{I}), E_{0,0}(\mathbb{F}_3)),\ N(\mathcal{I}) = 3,\ N(\mathcal{P}) < 100$$

$\mathcal{P}$	eigenvalue	
$3 \pm 2i$	1	1
$4 \pm i$	1	1
$6 \pm i$	1	1
$5 \pm 4i$	-1	1
$7 \pm 2i$	1	1
$6 \pm 5i$	1	1
$8 \pm 3i$	1	1
$8 \pm 5i$	1	1
$9 \pm 4i$	-1	-1

Dimension of space of Bianchi modular forms

	$K = \mathbb{Q}(\sqrt{-2})$		$K = \mathbb{Q}(\sqrt{-7})$	
k	$\dim H^1$	$\dim H^1_{cusp}$	$\dim H^1$	$\dim H^1_{cusp}$
0	1	0	1	0
1	1	0	1	0
2	1	0	1	0
3	2	1	1	0
4	1	0	2	1
5	3	2	2	1
6	2	1	2	1
7	4	3	3	2
8	2	1	3	2
9	5	4	3	2
10	3	2	4	3
11	6	5	4	3
12	3	2	6	5
13	7	6	5	4
14	4	3	5	4
15	8	7	5	4

Dimension formula (Known case: Grunewald et al.)

$$\dim H^1_{cusp}(\mathrm{SL}_2(\mathcal{O}_K), E_k) \geq \left(\frac{1}{24} \prod_{p \in \mathcal{R}} (p^{\nu_p} + 1) + c_2(-1)^{k+1} \right)(k+1)$$
$$-\nu_{K,k} \frac{h_K}{2} - 2^{|\mathcal{R}|-2} + c_4 \epsilon_{k+2} + c_3 \mu_{k+2} \quad + \quad \delta_{k,0}$$

where

- $c_2 = \begin{cases} 2^{|\mathcal{R}|-4} & p \equiv 1 \pmod 4 \text{ for all } p \in \mathcal{R},\ p \neq 2 \\ 0 & \text{otherwise} \end{cases}$
- $c_3 = \begin{cases} 2^{|\mathcal{R}|-1} & p^{\nu_p} \equiv 1 \pmod 3 \text{ for all } p \in \mathcal{R} \\ 2^{|\mathcal{R}|-2} & 3 \in \mathcal{R} \text{ and } p^{\nu_p} \equiv 1 \pmod 3 \text{ for all } p \in \mathcal{R},\ p \neq 3 \\ 0 & \text{otherwise} \end{cases}$
- $c_4 = \begin{cases} 2^{|\mathcal{R}|} & p \equiv 1 \text{ or } 3 \pmod 8 \text{ for all } p \in \mathcal{R} \\ 2^{|\mathcal{R}|-1} & 2 \in \mathcal{R} \text{ and } p^{\nu_p} \equiv 1 \text{ or } 3 \pmod 8 \text{ for all } p \in \mathcal{R},\ p \neq 2 \\ 0 & \text{otherwise} \end{cases}$
- $h_K = Cl(K)$
- $\nu_{K,k} = \begin{cases} 0 & K = \mathbb{Q}(\sqrt{-1}),\ k \equiv 0, 1 \pmod 3 \text{ or } K = \mathbb{Q}(\sqrt{-3}),\ k \equiv 0 \pmod 2 \\ 1 & \text{otherwise} \end{cases}$
- $\epsilon_k = \begin{cases} \frac{(-1)^{n/2}}{4} & k \equiv 0 \pmod 2 \\ 0 & \text{otherwise} \end{cases}$
- $\mu_k = \begin{cases} 0 & k \equiv 1 \pmod 3 \\ -\frac{1}{3} & k \equiv 2 \pmod 3 \\ \frac{1}{3} & \text{otherwise} \end{cases}$

Galois Side - Martinet Search

L/K: finite ext.
Searching number fields with prescribed ramification over K (unramified outside S: finite set of primes).

Let

$$f_{\alpha,K}(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n \in \mathcal{O}_K[x]$$

be the defining polynomial of L over K where

$$a_i = \sum_{1 \le j \le m} a_{ij}\omega_j, \; a_{ij} \in \mathbb{Z} .$$

$\rightarrow$ <u>Coefficients a_k are bounded</u> ($\rightarrow$ a_{ij}'s are bounded) .

Galois Side - Martinet Search

Theorem (Martinet, Driver)

K: Number field of degree m, L/K: relative ext. of degree n, d_K, d_L: discriminant of K, L respectively, $\sigma_1, \ldots, \sigma_m$: embeddings of K into $\mathbb{C}$.

Then there exists $\alpha \in \mathcal{O}_L \setminus \mathcal{O}_K$ s.t.

- *satisfies the following inequality:*

$$\sum_{1 \le i \le mn} |\alpha_i|^2 \le \frac{1}{n} \sum_{1 \le j \le m} \left|\sigma_j\left(\mathrm{Tr}_{L/K}(\alpha)\right)\right|^2 + \gamma_{m(n-1)} \left(\frac{|d_L|}{n^m |d_K|}\right)^{1/m(n-1)}$$

  where the α_i's are conjugates of α.

- *a_1 (coefficient of $f_{\alpha,K}$) can be chosen from a finite set of values $\subset \mathcal{O}_K$.*

Galois Side - Martinet Search

Theorem (Martinet, Driver)

- *a_1 (coefficient of $f_{\alpha,K}$) can be chosen from a finite set of values $\subset \mathcal{O}_K$.*

$$f_{\alpha,K}(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1}x + a_n \in \mathcal{O}_K[x]$$

$$a_1 \in \left\{ \sum_{1\le j\le m} a_{1j}\omega_j \;\middle|\; 0 \le a_{11} \le \left\lfloor \frac{n}{2} \right\rfloor,\ -\left\lfloor \frac{n-1}{2} \right\rfloor \le a_{1j} \le \left\lfloor \frac{n}{2} \right\rfloor \ (j \ge 2) \right\}$$

Choose a_1 and fix:

$$\sum_{1\le i\le mn} |\alpha_i|^2 \le \frac{1}{n} \sum_{1\le j\le m} |\sigma_j(a_1)|^2 + \gamma_{m(n-1)} \left(\frac{|d_L|}{n^m |d_K|} \right)^{1/m(n-1)} =: C_{a_1}$$

Galois Side - Martinet Search

Theorem (Driver)

- *Range of* a_n : $\displaystyle\sum_{1\le i\le m} |\sigma_i(a_n)|^2 \le \left(\frac{C_{a_1}}{n}\right)^n$
- *Range of* a_k $(2 \le k \le n-1)$: $\displaystyle s_k = \sum_{1\le j\le n} a_j^k$

  $a_i,\ s_i\ (1 \le i \le k-1)$ *: given*

  $$\overrightarrow{b} = -\sum_{1\le j\le k-1} a_{k-j}s_j\ ,\ \ \overrightarrow{a_k} = \frac{1}{k}\left(\overrightarrow{b} - \overrightarrow{s_k}\right)$$

  and s_k *can be bounded:*

  $$\sum_{1\le i\le m} |\sigma_i(s_k)|^2 \le C_{a_1}^k\ .$$

Galois Side - Martinet Search

Example: a_n's bound

$$-\frac{\sqrt{\frac{1}{2^{n-2}}\left(\frac{C_{a_1}}{n}\right)^n}}{(\omega-\overline{\omega})i} \leq a_{n2} \leq \frac{\sqrt{\frac{1}{2^{n-2}}\left(\frac{C_{a_1}}{n}\right)^n}}{(\omega-\overline{\omega})i}$$

and

$$\frac{-\sqrt{\frac{1}{2^{n-2}}\left(\frac{C_{a_1}}{n}\right)^n + (\omega-\overline{\omega})^2 a_{n2}^2} - (\omega+\overline{\omega})a_{n2}}{2} \leq a_{n1} \leq \frac{\sqrt{\frac{1}{2^{n-2}}\left(\frac{C_{a_1}}{n}\right)^n + (\omega-\overline{\omega})^2 a_{n2}^2} - (\omega+\overline{\omega})a_{n2}}{2}$$

Numerical Data

Result A

List of L which satisfies

- $\mathrm{Gal}(L/\mathbb{Q}) \simeq A_4$
- Unramified outside $S = \{2, 3\}$ over $\mathbb{Q}$

consists of 1 element:

- $P_L(x) = x^4 - 2x^3 + 6x^2 - 4x + 2$

$$\rho^{proj} : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{PSL}_2(\mathbb{F}_3)$$

$$\Rightarrow \quad \rho : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{SL}_2(\mathbb{F}_3)$$

$$\Rightarrow \quad \rho_K : \mathrm{Gal}(L/K) \to \mathrm{SL}_2(\mathbb{F}_3)$$ (Rosengren's idea)

Numerical Data : comparison

$\mathcal{P}$	$N(\mathcal{P})$	$\mathrm{Tr}(\rho_K(\mathrm{Frob}_{\mathcal{P}}))$	
$2+i$	5	1	-1
3	9	-1	-1
$3+2i$	13	1	1
$4+i$	17	1	1
$5+2i$	29	1	-1
$6+i$	37	1	1
$5+4i$	41	-1	1
7	49	-1	-1
$7+2i$	53	1	1
$6+5i$	61	1	1
$8+3i$	73	1	1
$8+5i$	89	1	1
$9+4i$	97	-1	-1

$\mathcal{P}$	eigenvalue	
$3\pm 2i$	1	1
$4\pm i$	1	1
$6\pm i$	1	1
$5\pm 4i$	-1	1
$7\pm 2i$	1	1
$6\pm 5i$	1	1
$8\pm 3i$	1	1
$8\pm 5i$	1	1
$9\pm 4i$	-1	-1

$$K=\mathbb{Q}(\sqrt{-1}),\ T(\mathcal{P}) \curvearrowright H^1(\Gamma_0(\mathcal{I}), E_{0,0}(\mathbb{F}_3))$$

Numerical Data

Result B

Lists of L which are unramified outside S over K (degree 5) :

K	S	# of L	$\mathrm{Gal}(L^g/\mathbb{Q})$
$\mathbb{Q}(\sqrt{-1})$	$\{2,3\}$	14	$T_5, T_{22}, T_{41}, T_{43}$
$\mathbb{Q}(\sqrt{-2})$	$\{2,3\}$	42	$T_5, T_{22}, T_{41}, T_{43}$
$\mathbb{Q}(\sqrt{-3})$	$\{2,3\}$	12	$T_5, T_{22}, T_{40}, T_{41}, T_{43}$
$\mathbb{Q}(\sqrt{-3})$	$\{3,11\}$	3	T_1, T_{11}
$\mathbb{Q}(\sqrt{-11})$	$\{3,11\}$	3	T_1, T_{11}
$\mathbb{Q}(\sqrt{-7})$	$\{7,11\}$	5	T_1, T_2, T_6, T_{22}
$\mathbb{Q}(\sqrt{-11})$	$\{7,11\}$	3	T_1, T_3, T_{22}

※ up to isom. ※ L^g: Galois closure of L over $\mathbb{Q}$

Numerical Data

Result C

From the lists of Result B: List of L which satisfies $\mathrm{Gal}(L/K) \simeq A_5$ consists of 4 elements:

- $K = \mathbb{Q}(\sqrt{-3})$, $S = \{3, 11\}$
  $x^5 + \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)x^4 + (-9 + 2\sqrt{3}i)x^3 - 3x^2 + (15 - 15\sqrt{3}i)x + (27 - 6\sqrt{3}i)$
- $K = \mathbb{Q}(\sqrt{-3})$, $S = \{3, 11\}$
  $x^5 + \left(-\frac{5}{2} + \frac{\sqrt{3}}{2}i\right)x^4 - \sqrt{3}ix^3 + \left(\frac{5}{2} + \frac{\sqrt{3}}{2}i\right)x^2 - 4x + \left(\frac{3}{2} - \frac{5\sqrt{3}}{2}i\right)$
- $K = \mathbb{Q}(\sqrt{-11})$, $S = \{3, 11\}$
  $$x^5 + \left(-\frac{5}{2} + \frac{\sqrt{11}}{2}i\right)x^4 + (8 - \sqrt{11}i)x^3 + \left(-\frac{19}{2} + \frac{17\sqrt{11}}{2}i\right)x^2 + (-32 - 8\sqrt{11}i)x + \left(\frac{35}{2} - \frac{7\sqrt{11}}{2}i\right)$$
- $K = \mathbb{Q}(\sqrt{-11})$, $S = \{3, 11\}$
  $x^5 + (-2 + \sqrt{11}i)x^4 + \left(\frac{1}{2} - \frac{5\sqrt{11}}{2}i\right)x^3 + (24 + 2\sqrt{11}i)x^2 + (-7 + 14\sqrt{11}i)x + (-32 - 2\sqrt{11}i)$

Future Works

- Construct $\rho_K : \mathrm{Gal}(L/K) \to \mathrm{SL}_2(\mathbb{F}_4)$ and compute $\mathrm{Tr}(\rho_K(\mathrm{Frob}_\lambda))$ from the Result C.
- Find more examples of "Matching".
- Extend the database of Hecke Side and Galois Side.

What's Magma?

- Computer Algebra Software package.
- Magma project has been headed by John Cannon (Univ. of Sydney) in Australia.
  - Designed to solve computationally hard problems in algebra, number theory, geometry, and combinatorics.
  - Not free but not for profit either.
- Reference:
  - Wieb Bosma and John Cannon, *Discovering Mathematics with Magma: Reducing the Abstract to the Concrete* (Algorithms and Computation in Mathematics)

Demonstration

$f(x) = x^4 - 2x^3 + 6x^2 - 4x + 2$ (from Result A)

> f:=x$^4 - 2 * x^3 + 6 * x^2 - 4 * x + 2;$

>> f:=x$^4 - 2 * x^3 + 6 * x^2 - 4 * x + 2;$
User error: Identifier 'x' has not been declared or assigned

Demonstration

$f(x) = x^4 - 2x^3 + 6x^2 - 4x + 2$ (from Result A)

```
> PA<x>:=PolynomialAlgebra(Rationals());
> f:=x^4 - 2*x^3 + 6*x^2 - 4*x + 2;
> N<a>:=NumberField(f);
> MinimalPolynomial(a) eq f;
true
> a^7;
-6*a^3 + 60*a^2 - 44*a + 24
> 3/a;
1/2*(-3*a^3 + 6*a^2 - 18*a + 12)
> GaloisGroup(N);
Permutation group acting on a set of cardinality 4
Order = 12 = 2^2*3
(1, 2)(3, 4)
(1, 2, 3)
...
```

Demonstration

Explicit isomorphism: $A_5 \simeq \mathrm{SL}_2(\mathbb{F}_4)$

```
> F<w>:=GF(4);
> H:=SL(2,F);
> G:=Alt(5);
> IsIsomorphic(G,H);
true Homomorphism of GrpPerm:
G, Degree 5, Order 2^2 * 3 * 5 into SL(2, GF(2,2)) induced by
(3, 4, 5) |--> [ 0 w]
[w^2 1]
(1, 2, 3) |--> [w^2 0]
[w^2 w]
>
```

Demonstration

- $K = \mathbb{Q}(\sqrt{-1})$
- $f(x) = x^5 + (-1 + 2\sqrt{-1})x^4 + (-6 + 2\sqrt{-1})x^2 + (-4 - 7\sqrt{-1})x - 3\sqrt{-1}$
- M: splitting field of f over K

$\rightarrow$ Check $\mathrm{Gal}(M/K) \simeq A_5$

```
> K<i>:=ext<Rationals()|Polynomial([1,0,1])>;
> MinimalPolynomial(i);
$.1^2 + 1
> _<x>:=PolynomialAlgebra(K);
> f:=x^5 + (-1 + 2*i)*x^4 + (-6 + 2*i)*x^2 + (-4 - 7*i)*x - 3*i;
> GaloisGroup(f);
Permutation group acting on a set of cardinality 5
Order = 60 = 2^2 * 3 * 5
(3, 4, 5)
(1, 2, 3)
[ 52*$.1^2 - 24*$.1 + O(13^2), 75*$.1^2 - 77*$.1 - 82 + O(13^2), 42*$.1^2 -
68*$.1 + 43 + O(13^2), 49 + O(13^2), 20 + O(13^2)]
GaloisData over Z _ Prime Ideal
Two element generators:
[13, 0]
[8, 1] - relative case
```

Demonstration

More info.

- Magma: Computer Algebra System
  http://magma.maths.usyd.edu.au/magma/
- Online Demo (20 seconds limit)
  http://magma.maths.usyd.edu.au/calc/