Computing with automorphic forms

Matthew Greenberg
University of Calgary

27 June 2011

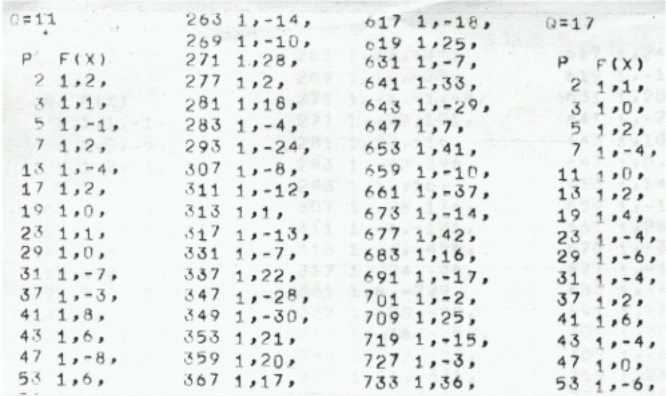
Outline

1. computing modular forms
   - history
2. modular symbols
3. algebraic modular forms (after Gross)
   - previous work by others
   - connection with class groups of lattices
4. lattice methods
   - isometry class enumeration using $\mathfrak{p}$-neighbours (after Kneser)
   - isomorphism testing – Plesken & Souvignier
5. $\mathfrak{p}$-neighbours and Hecke operators
6. to-do list

Introduction

Enumeration of automorphic forms has been an active domain since the 1970s.

Wada (1972) – T_p on $S_2(q)$, $q < 1000$ prime, 128 pages



Q=11						Q=17	
P	F(X)	263	1,-14,	617	1,-18,	P	F(X)
		269	1,-10,	619	1,25,		
2	1,2,	271	1,28,	631	1,-7,	2	1,1,
3	1,1,	277	1,2,	641	1,33,	3	1,0,
5	1,-1,	281	1,16,	643	1,-29,	5	1,2,
7	1,2,	283	1,-4,	647	1,7,	7	1,-4,
13	1,-4,	293	1,-24,	653	1,41,	11	1,0,
17	1,2,	307	1,-8,	659	1,-10,	13	1,2,
19	1,0,	311	1,-12,	661	1,-37,	19	1,4,
23	1,1,	313	1,1,	673	1,-14,	23	1,-4,
29	1,0,	317	1,-13,	677	1,42,	29	1,-6,
31	1,-7,	331	1,-7,	683	1,16,	31	1,-4,
37	1,-3,	337	1,22,	691	1,-17,	37	1,2,
41	1,8,	347	1,-28,	701	1,-2,	41	1,6,
43	1,6,	349	1,-30,	709	1,25,	43	1,-4,
47	1,-8,	353	1,21,	719	1,-15,	47	1,0,
53	1,6,	359	1,20,	727	1,-3,	53	1,-6,
		367	1,17,	733	1,36,		

The Antwerp tables (1972)

tables of elliptic curves, Mordell-Weil generators, Hecke eigenvalues, curves with conductor 2^a3^b, dimensions of rational eigenspaces of the Hecke algebra, supersingluar j-invariants

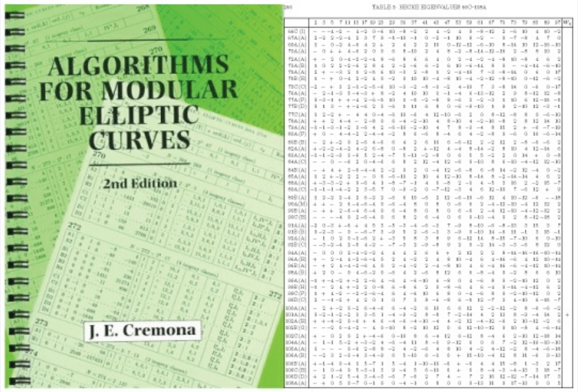
Table 3: Hecke eigenvalues (Vélu)

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	p	
11B	-2	-1	1	-2	-	4	-2	0	-1	0	7	3	-8	-6	8	-6	5	12	-7	-3	4	-10	-6	15	-7		11B
14C	+	-2	0	-	0	-4	6	2	0	-6	-4	2	6	8	-12	6	-6	8	-4	0	2	8	-6	-6	-10		14C
15C	-1	+	-	0	-4	-2	2	4	0	-2	0	-10	10	4	8	-10	-4	-2	12	-8	10	0	12	-6	2		15C
17C	-1	0	-2	4	0	-2	-	-4	4	6	4	-2	-6	4	0	6	-12	-10	4	-4	-6	12	-4	10	2		17C
19B	0	-2	3	-1	3	-4	-3	-	0	6	-4	2	-6	-1	-3	12	-6	-1	-4	6	-7	8	12	12	8		19B
20B	-	-2	+	2	0	2	-6	-4	6	6	-4	2	6	-10	-6	-6	12	2	2	-12	2	8	6	-6	2		20B
21B	-1	-	-2	+	4	-2	-6	4	0	-2	0	6	2	-4	0	6	12	-2	4	0	-6	-16	-12	-14	18		21B
24B	-	+	-2	0	4	-2	2	-4	-8	6	8	6	-6	4	0	-2	4	-2	-4	8	10	-8	-4	-6	2		24B
26D	-	-3	-1	1	-2	+	-3	6	-4	2	4	3	0	-5	13	12	-10	-8	-2	-5	-10	-4	0	6	14		26D
26B	+	1	-3	-1	6	-	-3	2	0	6	-4	-7	0	-1	3	0	-6	8	14	-3	2	8	12	-6	-10		26B
27B	0	-	0	-1	0	5	0	-7	0	0	-4	11	0	8	0	0	0	-1	5	0	-7	17	0	0	-19		27B
30A	+	-	+	-4	0	2	6	-4	0	-6	8	2	-6	-4	0	-6	0	-10	-4	0	2	8	12	18	2		30A
32B	-	0	-2	0	0	6	2	0	0	-10	0	-2	10	0	0	14	0	-10	0	0	-6	0	0	10	18		32B
33B	1	+	-2	4	-	-2	-2	0	8	-6	-8	6	-2	0	8	6	-4	6	-4	0	-14	-4	12	-6	2		33B
34A	-	-2	0	-4	6	2	+	-4	0	0	-4	-4	6	8	0	-6	0	-4	8	0	2	8	0	-6	14		34A
35B	0	1	+	-	-3	5	3	2	-6	3	-4	2	-12	-10	9	12	0	8	-4	0	2	-1	12	-12	-1		35B
36A	-	+	0	-4	0	2	0	8	0	0	-4	-10	0	8	0	0	0	14	-16	0	-10	-4	0	0	14		36A
37C	0	1	0	-1	3	-4	6	2	6	-6	-4	-	-9	8	3	-3	12	8	-4	-15	11	-10	9	6	8		37C
37A	-2	-3	-2	-1	-5	-2	0	0	2	6	-4	+	-9	2	-9	1	8	-8	8	9	-1	4	-15	4	4		37A
38A	-	-1	-4	3	2	-1	3	+	-1	-5	-8	-2	-8	4	8	-1	15	2	3	2	9	-10	-6	0	-2		38A

Modular symbol algorithm

modular symbols: formalism for studying the Hecke action on the homology of modular curves; introduced by Manin; reduction theory via continued fractions; algorithmic aspects developed by Merel and Cremona

Cremona's tables (1992-present)



Why compute spaces of automorphic forms?

- initially: testing the Shimura-Taniyama conjecture, i.e., the modularity of elliptic curves
- finding interesting number fields via Galois representations associated to modular forms
  - **Theorem.** (Dembélé, Dembélé-G-Voight, Skoruppa) There exist nonsolvable number fields unramified away from p for $p \in \{2, 3, 5, 7\}$.
  - The proof of the theorem uses explicit computations of Hilbert and Siegel modular forms.
- gathering evidence for various conjectures that comprise the Langlands program

Dembélé's field

A non-solvable Galois extension of $\mathbb{Q}$ ramified at 2 only

Lassina Dembélé

À la mémoire de ma sœur jumelle Fatouma. Déjà vingt ans que tu es partie

Abstract

In this paper, we show the existence of a non-solvable Galois extension of $\mathbb{Q}$ which is unramified outside 2. The extension K we construct has degree $251731094732800 = 2^{19}(3 \cdot 5 \cdot 17 \cdot 257)^2$ and has root discriminant $\delta_K < 2^{\frac{47}{8}} = 58.68...$, and is totally complex.

Résumé

Dans cet article, nous démontrons l'existence d'une extension galoisienne non résoluble de $\mathbb{Q}$ ramifiée seulement en 2. L'extension K que nous construisons est de degré $251731094732800 = 2^{19}(3 \cdot 5 \cdot 17 \cdot 257)^2$ et de discriminant normalisé $\delta_K < 2^{\frac{47}{8}} = 58,68...$, et est totalement complexe.

Roberts' polynomial

NONSOLVABLE POLYNOMIALS WITH FIELD DISCRIMINANT 5^A

DAVID P. ROBERTS

ABSTRACT. We present the first explicitly known polynomials in $\mathbf{Z}[x]$ with nonsolvable Galois group and field discriminant of the form $\pm p^A$ for $p \leq 7$ a prime. Our main polynomial has degree 25, Galois group of the form $PSL_2(5)^5.10$, and field discriminant 5^{69}. A closely related polynomial has degree 120, Galois group of the form $SL_2(5)^5.20$, and field discriminant 5^{311}. We completely describe 5-adic behavior, finding in particular that the root discriminant of both splitting fields is $125 \cdot 5^{-1/12500} \approx 124.984$ and the class number of the latter field is divisible by 5^4.

$$
\begin{aligned}
g_{25}(x) = {} & \\
& x^{25} - 25x^{22} + 25x^{21} + 110x^{20} - 625x^{19} + 1250x^{18} - 3625x^{17} + 21750x^{16} \\
& -57200x^{15} + 112500x^{14} - 240625x^{13} + 448125x^{12} - 1126250x^{11} + 1744825x^{10} \\
& -1006875x^{9} - 705000x^{8} + 4269125x^{7} - 3551000x^{6} + 949625x^{5} - 792500x^{4} \\
& +1303750x^{3} - 899750x^{2} + 291625x - 36535.
\end{aligned}
$$

Magma and Sage implementations (Stein)

- implementations of modular symbol packages in Magma, Sage
- data about $\Gamma_0(N)$-newforms of conductor ≤ 10000

Researchers can experiment!

```
> S := NewSubspace(CuspidalSubspace(ModularSymbols(353,2,+1)));
> S;
Modular symbols space for Gamma_0(353) of weight 2 and dimension
29 over Rational Field
> Decomposition(S,5);
[
    Modular symbols space for Gamma_0(353) of weight 2
    and dimension 1 over Rational Field,
    Modular symbols space for Gamma_0(353) of weight 2
    and dimension 3 over Rational Field,
    Modular symbols space for Gamma_0(353) of weight 2
    and dimension 11 over Rational Field,
    Modular symbols space for Gamma_0(353) of weight 2
    and dimension 14 over Rational Field
]
```

- High level languages like Magma and Sage have lots of carefully implemented, optimized algebraic and number theoretic functionality built in.
    - lattice algorithms, group theory, fast linear algebra, ...
- This facilitates experimentation for those of us who don't know anything about serious computer programming.

Computing $M_2(\Gamma_0(N))$

- Each $f \in M_2(\Gamma_0(N))$ has a Fourier expansion:

$$f(z) = \sum_{n \geq 0} a_n(f) q^n, \qquad q = e^{2\pi i z}.$$

- $a_n(f) = a_n(g) \; \forall \; n \leq B(N) \sim \frac{2}{12}[\Gamma_0(1) : \Gamma_0(N)] \implies f = g$.
- To represent $M_2(\Gamma_0(N))$ on a computer, we could store the first $B(N)$ Fourier coefficients of a basis of $M_2(\Gamma_0(N))$.

Computing $M_2(\Gamma_0(N))$ as a Hecke-module

- $M_2(\Gamma_0(N))$ admits the action of a commutative algebra of *Hecke operators*

$$\mathbb{T} = \langle T_p : p \text{ prime} \rangle \subset \operatorname{End}_{\mathbb{C}} M_2(\Gamma_0(N)),$$

$$(f|T_p)(z) = \frac{1}{p}\sum_{a=0}^{p-1} f\left(\frac{z+a}{p}\right) + pf(pz)$$

- Suppose f is a $\mathbb{T}$-eigenvector.
  - If $a_0 \neq 0$, then

$$f|T_p = a_p(f)f, \quad a_p(f) = p+1$$

  - If $a_0 = 0$ and $a_1 = 1$, then

$$f|T_p = a_p(f)f, \quad |a_p| \leq 2\sqrt{p}$$

Modular symbols (Manin, Mazur, Merel, . . .)

- $\Delta := \mathrm{Div}\,\mathbb{P}^1(\mathbb{Q})$, $\Delta^0 := \mathrm{Div}^0\,\mathbb{P}^1(\mathbb{Q})$
- $\mathrm{MS}_N = \mathrm{MS}_N(\mathbb{C}) := \mathrm{Hom}_{\Gamma_0(N)}(\Delta^0, \mathbb{C})$,

$$\mathrm{MS}_N^+ = \mathrm{MS}_N^+(\mathbb{C}) := \Big\{\varphi \in \mathrm{MS}_N : \varphi\left(\{\left(\begin{smallmatrix} -1 & \\ & 1 \end{smallmatrix}\right) y\} - \{\left(\begin{smallmatrix} -1 & \\ & 1 \end{smallmatrix}\right) x\}\right) = \varphi(\{y\} - \{x\})\Big\} \subset \mathrm{MS}_N$$

- The Hecke operators act on MS_N and MS_N^+

$$(\varphi | T_p)(\{y\} - \{x\}) := \sum_{a=0}^{p-1} \varphi\left(\left\{\left(\begin{smallmatrix} 1 & a \\ & p \end{smallmatrix}\right) y\right\} - \left\{\left(\begin{smallmatrix} 1 & a \\ & p \end{smallmatrix}\right) x\right\}\right) + \varphi\left(\left\{\left(\begin{smallmatrix} p & 0 \\ & 1 \end{smallmatrix}\right) y\right\} - \left\{\left(\begin{smallmatrix} p & 0 \\ & 1 \end{smallmatrix}\right) x\right\}\right) \qquad (p \nmid N).$$

- **Theorem.** The Hecke-modules $M_2(\Gamma_0(N))$ and MS_N^+ are isomorphic.
- If $e : \Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q}) \to \mathbb{C}$, define the *boundary symbol*

$$\varphi_e(\{y\} - \{x\}) := e(y) - e(x), \quad \mathrm{BS}_N := \{\text{such } \varphi_e\} \subset \mathrm{MS}_N^+ .$$

- Define the *Eichler-Shimura map* $\mathrm{ES}^+ : S_2(\Gamma_0(N)) \to \mathrm{MS}^+$ by

$$\mathrm{ES}^+(f)(\{y\} - \{x\}) = \pi i \left(\int_x^y + \int_{-x}^{-y} \right) f(z) dz.$$

- **Theorem.** The induced map

$$\mathrm{ES}^+ : S_2(\Gamma_0(N)) \longrightarrow \mathrm{MS}^+ / \mathrm{BS}$$

is an isomorphism.

Computing MS_N

- **Theorem.** $\Delta^0 = \mathrm{Div}^0 \mathbb{P}^1(\mathbb{Q})$ is a finitely generated $\mathbb{Z}[\Gamma_0(N)]$-module.
- If
$$\Delta^0 = \mathbb{Z}[\Gamma_0(N)]D_i + \cdots + \mathbb{Z}[\Gamma_0(N)]D_i,$$
then $\varphi \in \mathrm{MS}$ is determined by the h numbers $\varphi(D_i)$.
- We must *enumerate* generators D_i
- We need a *reduction theory*: Given $D \in \Delta^0$, find $w_i \in \mathbb{Z}[\Gamma_0(N)]$ such that
$$D = w_1 D_1 + \cdots w_h D_h.$$

Enumeration and reduction

- We say $x = (a : c)$ and $y = (b : d)$ are *adjacent* if
$$ad - bc = \pm 1.$$
- The action of $\Gamma_0(N)$ on Δ^0 preserves adjacency the natural map
$$\Gamma_0(N)\backslash\{\text{adjacent pairs}\} \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$$
is an isomorphism.
- For $(\bar{b} : \bar{d}) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, define
$$D_{(\bar{b}:\bar{d})} = \{(b : d)\} - \{(a : c)\}, \qquad ad - bc = \pm 1.$$

$$D_{(\bar{b}:\bar{d})} = \{(b:d)\} - \{(a:c)\}, \qquad ad - bc = \pm 1.$$

- Enumeration: $\{D_{(\bar{b}:\bar{d})}\}$ generates Δ^0 as a $\Gamma_0(N)$-module.
- If $x, y \in \mathbb{P}^1(\mathbb{Q})$, there is a sequence

$$x = x_0, x_1, \ldots, x_n = y, \qquad x_j = (p_j : q_j),$$

  such that $p_{j-1}q_j - q_{j-1}p_j = \pm 1$ are adjacent.
- Reduction: We may take p_j/q_j to be the j-th convergent in the continued fraction expansion of x.
- Thus, the reduction theory is just the continued fraction algorithm.

- All approaches to computing spaces of automorphic forms involve enumeration and reduction steps.

Adelic automorphic forms

- Let F be a totally real number field and set $G = \mathrm{GL}_n$.
- Define *adele rings*

$$\mathbb{A}_f = \left\{ x \in \prod_{v \nmid \infty} F_v : x_v \in \mathcal{O}_{F,v} \text{ for almost all } v \right\},$$

$$F_\infty = \prod_{v \mid \infty} F_v,$$

$$\widehat{\mathcal{O}}_F = \prod_{v \nmid \infty} \mathcal{O}_{F,v}$$

- Set
$$G_\infty = G(F_\infty).$$
- Let $K_f \subset G(\widehat{\mathcal{O}}_F)$ be an open subgroup, e.g.,
$$K_f = K_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G(\widehat{\mathcal{O}}_F) : c \in \mathcal{N}\widehat{\mathcal{O}}_F \right\}, \quad \mathcal{N} \subset \mathcal{O}_F.$$
- Let K_∞ be a maximal compact, connected subgroup of $G(\mathbb{R})$. $(K_\infty = \mathrm{SO}(n))$
- Define the *Shimura manifold of level K_f*:
$$Y(K_f) = G(\mathbb{Q})\backslash\Big(G(\mathbb{A}_f)/K_f \times \underbrace{G_\infty/K_\infty Z_\infty}_{\mathfrak{H}}\Big).$$

$$Y(K_f) = G(F)\backslash\Big(G(\mathbb{A}_f)/K_f \times \mathfrak{H}\Big).$$

- **Theorem:** $h(K_f) := |G(F)\backslash G(\mathbb{A}_f)/K_f| < \infty$
- Sorting out the diagonal action,

$$Y(K_f) = \coprod_{i=1}^{h(K_f)} \Gamma_{x_i}\backslash\mathfrak{H}$$

where

$$G(\mathbb{A}_f) = \coprod_{i=1}^{h(K_f)} G(F)x_iK_f, \qquad \Gamma_{x_i} := G(F) \cap x_iK_fx_i^{-1}.$$

- $G = \mathrm{GL}_1$, $K_f = 1 + \mathcal{N}\mathcal{O}_F$,

$$X(K_f) = \mathbb{A}_f^\times / F^\times (1 + \mathcal{N}\widehat{\mathcal{O}}_F) = \begin{array}{c}\text{ray class group}\\ \text{of conductor } \mathcal{N}\end{array}$$

- $F = \mathbb{Q}$, $G = \mathrm{GL}_2$, $K_f = K_0(N)$,

$$\det : G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K_f \xrightarrow{\sim} \mathbb{A}_f^\times/\mathbb{Q}^\times \widehat{\mathbb{Z}}^\times = \mathrm{Cl}(\mathbb{Q}) = \{1\},$$

$$\Gamma = K_f \cap GL_2(\mathbb{Q}) = \Gamma_0^\pm(N), \qquad \mathfrak{H} = \mathfrak{h}^\pm,$$

$$Y(K_f) = \Gamma_0^\pm(N)\backslash \mathfrak{h}^\pm = \Gamma_0(N)\backslash \mathfrak{h} = Y_0(N).$$

Hilbert modular varieties

- $G = \mathrm{GL}_2$, F totally real, $Y(K_f)$ is a *Hilbert modular variety*.
- If F has narrow class number one and $K_f = \mathrm{GL}_2(\widehat{\mathcal{O}}_F)$, then
$$Y(K_f) = \mathrm{SL}_2(\mathcal{O}_F)\backslash\mathfrak{h}^n \qquad (\dim_{\mathbb{R}} Y(K_f) = 2n).$$
- Computational challenge: Compute the systems of Hecke eigenvalues occurring in
$$H^i(Y(K_f), \mathbb{C})$$
- Most interesting: $i = n$; as $H^i(Y(K_f), \mathbb{C}) = 0$ for $i > 2n$, we call n the *middle dimension*.

Approaches to computing with Hilbert modular varieties

- Hybrid geometric/arithmetic methods, nice resolutions – the Sharbly complex
  - Gunnells, Yasaki
- Automorphic methods using functoriality, Jacquet-Langlands correspondence
  - Find systems of Hecke-eigenvalues occurring in the cohomology of Hilbert modular varieties with systems occurring in spaces of *algebraic modular forms*.
  - Démbele, Donnelly, G, Voight

Algebraic modular forms

- introduced by Gross (Israel J. Math., 1999)
- a class of automorphic forms particularly well-suited to calculation

Setting

- $G/\mathbb{Q}$ connected, reductive algebraic group, $G(\mathbb{R})$ compact
  - e.g., definite orthogonal groups, definite unitary groups
- $K_f \subset G(\mathbb{A}_f)$ compact open subgroup

- Since $G(\mathbb{R})$ is compact, we take $K_\infty = G(\mathbb{R})$.

$$Y(K_f) = G(\mathbb{Q}) \backslash G(\mathbb{A}_f)/K_f \qquad \text{(finite, size } h(K_f))$$

- 0-dimensional Shimura variety

- Let V be a finite-dimensional, algebraic representation of $G_{/\mathbb{Q}}$.

Space of algebraic modular forms, level K, weight V

$$M(V, K_f) = \{f : G(\mathbb{A}_f)/K_f \to V : f(\gamma g) = \gamma f(g),\ \gamma \in G(\mathbb{Q})\}$$

- Suppose

$$G(\mathbb{A}_f) = \coprod_{i=1}^{h} (K_f) G(\mathbb{Q}) x_i K_f$$

- $f \in M(V, K)$ determined by $\{f(x_i)\}$
- If we can represent elements of V, we can represent elements of $M(V, K)$ – provided we can find representatives $\{x_i\}$. We need an *enumeration algorithm*.

The Jacquet-Langlands correspondence

- Let F be a totally real field of even degree n, let B be the quaternion F-algebra ramified at the infinite places of F. Let R be a maximal order of B.
- Let $G = B^\times$ and let $K_f = (R \otimes \widehat{\mathcal{O}}_F)^\times$.

Theorem:

The same systems of Hecke eigenvalues occur in the two modules

$$H^n_{\text{cusp}}(Y(\mathrm{GL}_2(\widehat{\mathcal{O}}_F)), \mathbb{C}) \qquad \text{and} \qquad M(K_f, V_{\text{triv}}).$$

The multiplicities of these systems in $H^n_{\text{cusp}}(Y(\mathrm{GL}_2(\widehat{\mathcal{O}}_F)), \mathbb{C})$ and $M(K_f, V_{\text{triv}})$ are 2^n and 1, respectively.

- We can compute Hilbert modular forms via algebraic modular forms!

Hecke operators

$$f \in M(V,K) \longleftrightarrow \{f(g_1),\dots,f(g_h)\}$$

- p prime, $\varpi \in G(\mathbb{Q}_p) \hookrightarrow G(\mathbb{A}_f)$, $K_f \varpi K_f = \coprod_i \varpi_i K_f$
- Define $T(\varpi) : M(V,K_f) \to M(V,K_f)$ by

$$(f|T(\varpi))(xK_f) = \sum_i f(x\varpi_i K_f)$$

Knowing $\{f(g_i)\}$, how do we compute $(f|T(\varpi))(g_i)$?

- $g_i \varpi_j K_f = \gamma_{i,j} g_{k(i,j)} K_f$ for some $\gamma_{i,j} \in G(\mathbb{Q})$
- $G(\mathbb{Q})$-equivariance of $f \Rightarrow (f|T(\varpi))(g_i) = f(g_{k(i,j)})$.
- To compute $\gamma_{i,j}$, $g_{k(i,j)}$, we need a *reduction algorithm*.

Previous work

- Lansky & Pollack – $G = G_2$ over $\mathbb{Q}$
  - key fact: $G_2(\mathbb{Q})G_2(\widehat{\mathbb{Z}}) = G_2(\mathbb{A}_f)$
- Dembélé, Dembélé & Donnelly – $F/\mathbb{Q}$ totally real, B/F totally definite quaternion algebra, $G = B^*$
  - principal ideal testing/ideal principalization
- Cunningham, Dembélé – $B = \mathbb{H} \otimes \mathbb{Q}(\sqrt{5})$, $G = \mathrm{GU}_2(B)$
- Loeffler – $U(3)$ relative to $\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$
  - some clever "ad-hoc" methods

My goal

- Develop unified approach, systematic algorithms for computing with algebraic modular forms based on *lattice algorithms*.
- Implement them.

Rest of the talk:

- I'll describe some progress with orthogonal and (maybe) unitary groups.
- For these, I can compute Hecke operators on algebraic modular forms at *split primes* when $K_f = G(\widehat{\mathbb{Z}})$.

Orthogonal groups

- Let

$$q : \mathbb{Z}^m \times \mathbb{Z}^n \to \mathbb{Z}$$

  be a positive-definite, symmetric bilinear form.

- Let Q be its matrix and, for a $\mathbb{Z}$-algebra R, define

$$O(Q)(R) = \{A \in \mathrm{GL}_n(R) : AQA^t = Q\}.$$

- Since Q is positive-definite, $O(Q)(\mathbb{R}) \cong O(m)$ is compact.
- Thus, we may consider algebraic modular forms for

$$G := O(Q).$$

Split, even orthogonal groups (local theory)

- Suppose
$$q(x,x) = x_1^2 + x_2^2, \qquad Q = I.$$
- Suppose $p \equiv 1 \pmod 4$ and let $i \in \mathbb{Q}_p$ be a square root of -1. Setting
$$u_1 = x_1 + ix_2, \qquad u_2 = x_1 - ix_2,$$
we have
$$q(u,u) = u_1 u_2, \qquad Q \sim_{\mathbb{Q}_p} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$
- A 2-dimensional quadratic space equipped with the quadratic form $q(u,u) = u_1 u_2$ is called a *hyperbolic plane*.
- An (even) orthogonal group associated to a direct sum of hyperbolic planes is called *split*.

- Suppose $G = O(Q)$, where

$$Q = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}.$$

- Then for any field extension E of $\mathbb{Q}$,

$$G(E) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GL}_{2n}(E) : \begin{matrix} A^t B \text{ and } C^t D \text{ skew symmetric,} \\ A^t D + B^t C = I_n \end{matrix} \right\},$$

$$T(E) = \left\{ \begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix} \in G(E) : A \text{ diagonal} \right\},$$

$$B(E) = \left\{ \begin{pmatrix} A & B \\ 0 & {}^tA^{-1} \end{pmatrix} \in G(E) : \begin{matrix} A \text{ diagonal,} \\ A^t B \text{ skew-symmetric} \end{matrix} \right\}.$$

- We say that $e_1, \ldots, e_n, f_1, \ldots, f_n$ is a *Witt basis* of V if each pair $\{e_i, f_i\}$ spans a hyperbolic plane.

- **Theorem:** (Invariant factors) Let L and M be two unimodular lattices in $\mathbb{Q}_p^{2n}$. Then there is

$$e_1, \ldots, e_n, f_1, \ldots, f_n$$

of L, and integers

$$a_1 \geq a_2 \geq \cdots \geq a_n \geq 0,$$

such that

$$p^{a_1} e_1, \ldots, p^{a_n} e_n, p^{-a_1} f_1, \ldots, p^{-a_n} f_n$$

is a Witt basis of M.

- **Corollary:** $G(\mathbb{Q}_p)$ acts transitively on the set of unimodular lattices $L \subset \mathbb{Q}_p^{2n}$.

- Let

$$\begin{aligned} K_p &= \mathrm{GL}_{2n}(\mathbb{Z}_p) \cap G(\mathbb{Q}_p), \\ \Delta^+ &= \{\mathrm{diag}(p^{a_1}, \ldots, p^{a_n}, \pi^{-a_1}, \ldots, p^{-a_n}) : a_1 \geq \cdots a_n\} \\ &\qquad \subset T(\mathbb{Q}_p). \end{aligned}$$

- **Corollary:** (p-adic Cartan decomposition) Let $g \in G(\mathbb{Q}_p)$. Then the double coset $K_p g K_p$ contains a unique element of Δ^+.

Let

$$P = \mathrm{diag}(p, 1, \ldots, 1, p^{-1}, 1, \ldots, 1) \in \Delta^+.$$

The following sets are in canonical bijection:

1. $K_p P K_p / K_p$,
2. the set of lattices in $\mathbb{Q}_p^{2n}$ with invariant factors $p, p^{-1}, 1, \ldots, 1$ with respect to $\mathcal{L}_p = \mathbb{Z}_p^{2n}$.
3. the set of isotropic lines in $\mathcal{L}_p / p\mathcal{L}_p$,
4. the set of $\mathbb{F}_p$-rational points of the hypersurface $V(q) \subset \mathbb{P}^{2n-1}$.

Lattices (global theory)

Equivalence and local equivalence

Let L and M be lattices in $V = \mathbb{Q}^m$.

- L and M are *equivalent* if there is a linear isomorphism $f : L \to M$ such that

$$q(f(x), f(y)) = q(x, y).$$

- L and M are *locally equivalent* if, for each p, there is a linear isomorphism $f_p : L \otimes \mathbb{Z}_p \to M \otimes \mathbb{Z}_p$ such that

$$q(f_p(x), f_p(y)) = q(x, y).$$

- Clearly, equivalence implies local equivalence.

The genus of a lattice

- The *genus* of a lattice L in V, written $\operatorname{gen} L$, is the local equivalence class of L.
- Given unimodular $L_p \subset V \otimes \mathbb{Q}_p$ for each p such that $L_p = \mathbb{Z}_p^m$ for all but finitely many p, then there is a unique lattice L such that $L \otimes \mathbb{Z}_p = L_p$ for all p.
- If L_p and M_p are unimodular lattices in $V \otimes \mathbb{Q}_p$, then there is a matrix $A_p \in O(Q)(\mathbb{Q}_p)$ such that $AL_p = M_p$.

Adelic description of the genus of $L_* := \mathbb{Z}^m$

- $\operatorname{gen} L_* = G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}})$
- $G(\mathbb{Q})\backslash \operatorname{gen} L_* = G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}})$
- $h(L_*) = h(\operatorname{gen} L_*) := |G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}})|$

Lattice enumeration – Kneser's method

Enumeration of quadratic forms in n variables

Vol. VIII, 1957 241

Klassenzahlen definiter quadratischer Formen

Von Martin Kneser in Heidelberg

Satz 3. *Die Klassenzahl $h(n, d)$ der positiv definiten quadratischen Formen in n Veränderlichen mit der Diskriminante d hat für $d \leq 3$, $n + d \leq 17$ die Werte:*

n =	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
d = 1	1	1	1	1	1	1	1	2	2	2	2	3	3	4	5	8
d = 2	1	1	1	1	1	1	2	2	3	3	4	4	6	7	11	
d = 3	1	2	2	2	2	3	3	4	5	7	8	10	13	19		

- Scharlau & Hemkemeyer, Math. Comp. (1998) – implementation of Kneser's method as an algorithm, large scale computations

p-neighbours

- Lattices L and M in $\mathbb{Q}^{2n}$ are called *p-neighbours* if $L \cap M$ has index p in both L and M.
- **Theorem.** Suppose $x \in L - pL$ and $q(v, v) \in p^2\mathbb{Z}$. Then

  $$L(x) := \{y \in L : q(x, y) \in p\mathbb{Z}\} + p^{-1}x$$

  is a p-neighbour of L. All p-neighbours arise in this fashion, and $L(x)$ is completely determined by the line of class of x in L/pL. Finally, $L(x) \in \operatorname{gen} L$.
- **Theorem.** You can compute $\operatorname{gen} L$ by computing p-neighbours for enough p.

Suppose (V, Q) is split at p. Let

$$P = \mathrm{diag}(p, 1, \ldots, 1, p^{-1}, 1, \ldots, 1) \in \Delta^+.$$

The following sets are in canonical bijection:

1. KPK/K, where $K = G(\widehat{\mathbb{Z}})$,
2. the set of unimodular lattices in $\mathbb{Q}^{2n}$ with invariant factors at p equal to $p, p^{-1}, 1, \ldots, 1$ with respect to $\mathbb{Z}_p^{2n}$.
3. the set of isotropic lines in L_*/pL_*,
4. the set of $\mathbb{F}_p$-rational points of the hypersurface $V(q) \subset \mathbb{P}^{2n-1}$,
5. p-neighbours of L_*.

Hecke operators for $G = O(q)$ at split p

$$f \in M(V, K) \longleftrightarrow \{f(g_1), \ldots, f(g_h)\}$$

- $\varpi \in G(\mathbb{Q}_p) \hookrightarrow G(\mathbb{A}_f)$, $K_f \varpi K_f = \coprod_i \varpi_i K_f$
- Define $T(\varpi) : M(V, K_f) \to M(V, K_f)$ by

$$(f|T(\varpi))(xK_f) = \sum_i f(x\varpi_i K_f)$$

Knowing $\{f(g_i)\}$, how do we compute $(f|T(\varpi))(g_i)$?

- $g_i \varpi_j K_f = \gamma_{i,j} g_{k(i,j)} K_f$ for some $\gamma_{i,j} \in G(\mathbb{Q})$
- $G(\mathbb{Q})$-equivariance of $f \Rightarrow (f|T(\varpi))(g_i) = f(g_{k(i,j)})$.
- To compute $\gamma_{i,j}$, $g_{k(i,j)}$, we need a *reduction algorithm*.

Reduction

- We must be able to test lattices for isomorphism.
- algorithm due to Plesken and Souvignier
- matches up short vectors
- also used to compute automorphism group of a lattice

Unitary groups associated to CM fields

- $K/\mathbb{Q}$ imaginary quadratic
- For simplicity, assume $\mathcal{O}_K$ is a PID.
- For a $\mathbb{Q}$-algebra A, define

$$G(A) = \{x \in \mathrm{GL}_n(K \otimes A) : x\bar{x}^t = 1\}.$$

- K imaginary $\Rightarrow \mathrm{GL}_n(K \otimes \mathbb{R}) = \mathrm{GL}_n(\mathbb{C})$

$$G(\mathbb{R}) = \{x \in \mathrm{GL}_n(\mathbb{C}) : x\bar{x}^t = 1\} = U(n)$$

- $G(\mathbb{R}) = U(n)$ is compact
- p split in $K \Rightarrow$

$$G(\mathbb{Q}_p) = \{(x, y) \in \mathrm{GL}_n(K \otimes \mathbb{Q}_p) = \mathrm{GL}_n(\mathbb{Q}_p)^2 : \\ (x, y)(y^t, x^t) = 1\} = \mathrm{GL}_n(\mathbb{Q}_p), \quad (x, y) \longleftrightarrow y$$

X_K and Hermitian lattices

- (K^n, H) nondegenerate Hermitian space:

$$H : K^n \times K^n \to K, \quad H(x,y) = \sum_{i=1}^{n} x_i \bar{y}_i$$

- $\mathcal{L} := \{\text{Hermitian lattices in } K^n\}$
- standard lattice: $L_0 = \mathcal{O}_K^n \in \mathcal{L}$
- $G(\mathbb{A}_f)$ acts on $\mathcal{L}$:

$$g \cdot L = \text{unique } M \subset K^n \text{ such that } M_v = g_v L_v \text{ for all } v$$

- $K := \mathrm{stab}_{G(\mathbb{A}_f)} L_0$ is a maximal compact subgroup of $G(\mathbb{A}_f)$.
- Define the *genus of* L_0 by $\mathrm{gen}\, L_0 := G(\mathbb{A}_f) \cdot L_0$.

$$G(\mathbb{A}_f)/K \longleftrightarrow \mathrm{gen}\, L_0$$

Equivalence of Hermitian lattices

- We write $L \equiv M$ if $\gamma L = M$ for some $\gamma \in G(\mathbb{Q})$.
- $\operatorname{cl} L :=$ equivalence class of L

Fundmental finiteness theorem

Every genus of Hermitian lattices in K^n is the union of finitely many equivalence classes.

$$X_K = G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K \longleftrightarrow G(\mathbb{Q})\backslash \operatorname{gen} L_0 = \{\operatorname{cl} L_0, \dots, \operatorname{cl} L_h\}$$

- $h =$ class number of L_0
- Enumeration problem: Find representatives $L_1, \dots, L_h$ for the equivalence classes in $\operatorname{gen} L_0$

Lattice enumeration – Kneser's method

Enumeration of quadratic forms in n variables

Vol. VIII, 1957

Klassenzahlen definiter quadratischer Formen

Von Martin Kneser in Heidelberg

Satz 3. *Die Klassenzahl $h(n, d)$ der positiv definiten quadratischen Formen in n Veränderlichen mit der Diskriminante d hat für $d \leq 3$, $n + d \leqq 17$ die Werte:*

n =	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
d = 1	1	1	1	1	1	1	1	2	2	2	2	3	3	4	5	8
d = 2	1	1	1	1	1	1	2	2	3	3	4	4	6	7	11	
d = 3	1	2	2	2	2	3	3	4	5	7	8	10	13	19		

- Scharlau & Hemkemeyer, Math. Comp. (1998) – implementation of Kneser's method as an algorithm, large scale computations

- Hoffman, Manuscripta Math. (1991) – variant of Kneser's method for unitary groups, calculations by hand (?)
- Schiemann, J. Symbolic Comput. (1998) – computer implementation of unitary variant of Kneser's method, large scale computations

Class numbers of Hermitian lattices

Table 1.

Δ	h	H	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}
-3	1	I	1	1	1	1	2	2	3	4	6
							(2)	(1)	(2)	(2)	(2)
-4	1	I	1	1	1+1	2	3	4	6+3	12	25
					(1)(2)	(1)	(2)	(2)	(2)(2)	(2)	(2)
-7	1	I	1	2	3	5	11	26	71	291	2225
				(2)	(2)	(2)	(2)	(2)	(2)	(3)	(4)
-8	1	I	1+1	2	3+2	7	15+5	38	142+26		
			(1)(2)	(1)	(2)(2)	(2)	(2)(2)	(2)	(3)(4)		
-11	1	I	2	2	6	10	39	112	1027		
			(2)	(1)	(2)	(3)	(3)	(3)	(4)		
-15	2	I	2	5	14	48	238	2120			
			(2)	(2)	(2)	(3)	(3)	(4)			
		$I \perp \langle 2 \rangle$	2	5	14	48	240	2120			
			(2)	(2)	(3)	(3)	(4)	(4)			
-19	1	I	2	3	12	32	290	5225			
			(2)	(2)	(3)	(3)	(4)	(4)			
-20	2	I	3	6	18+13	98	879				
			(2)	(3)	(3)(4)	(3)	(4)				
		$I \perp \langle 2 \rangle$	1+2	6	21	98	773+158				
			(1)(2)	(2)	(2)	(3)	(4)(4)				
-23	3	I	9	30	126	768	8895				

$\mathfrak{p}$-neighbours

- Suppose p splits in K, $p = \mathfrak{p}\bar{\mathfrak{p}}$.
- *M is a $\mathfrak{p}$-neighbour of L* if there is a basis $\{v_i\}$ of L such that

$$M = \bar{\mathfrak{p}}\mathfrak{p}^{-1} v_1 \oplus \mathcal{O}_K v_2 \oplus \cdots \oplus \mathcal{O}_K v_{n-1} \oplus \mathcal{O}_K v_n.$$

Constructing $\mathfrak{p}$-neighbours

- Let $\{x_i\} \in \bar{\mathfrak{p}} L$ be representatives for $\mathbb{P}(\bar{\mathfrak{p}} L / pL) \approx \mathbb{P}^{n-1}(\mathbb{F}_p)$.
- Set

$$L(x_i) = \mathfrak{p}^{-1} x_i + \{y \in L : H(x_i, y) \in \mathfrak{p}\}$$

- The $L(x_i)$ are well defined and distinct.
- They are the $\mathfrak{p}$-neighbours of L.

$\mathfrak{p}$-neighbour of L associated to $x \in \bar{\mathfrak{p}}L - pL$

$$L(x) = \mathfrak{p}^{-1}x + \underbrace{\{y \in L : H(x,y) \in \mathfrak{p}\}}_{L_x}$$

Example: Let $\pi \in \mathfrak{p} - \mathfrak{p}^2$. Then

$$L = L_0, \quad x = (\bar{\pi}, 0, \ldots, 0), \quad L(x) = \bar{\mathfrak{p}}\mathfrak{p}^{-1} \oplus \mathcal{O}_K^{n-1}$$

- $(\bar{\pi}/\pi, 0, \ldots, 0)$ generates $L(x)/L \cap L(x) \approx \mathbb{Z}/p\mathbb{Z}$.
- $(1, 0, \ldots, 0)$ generates $L/L \cap L(x) = L/L_x \approx \mathbb{Z}/p\mathbb{Z}$.

Properties of $\mathfrak{p}$-neighbours

If M is a $\mathfrak{p}$-neighbour of L, we write $L \overset{\mathfrak{p}}{\rightsquigarrow} M$.

- $L \overset{\mathfrak{p}}{\rightsquigarrow} M \Leftrightarrow M \overset{\bar{\mathfrak{p}}}{\rightsquigarrow} L$
- $L \overset{\mathfrak{p}}{\rightsquigarrow} M \Rightarrow M \in \operatorname{gen} L$
- $M \in \operatorname{gen}^0 L$ (special genus) $\Rightarrow$

$$L = L_0 \overset{\mathfrak{p}}{\rightsquigarrow} L_1 \overset{\mathfrak{p}}{\rightsquigarrow} \cdots \overset{\mathfrak{p}}{\rightsquigarrow} L_t = M' \equiv M$$

- If K is a PID, then $\operatorname{gen}^0 L = \operatorname{gen} L$ and every class $[M] \in \operatorname{gen} L$ can be connected to L by a chain of $\mathfrak{p}$-neighbours.

Enumeration algorithm

- keep generating $\mathfrak{p}$-neighbours, testing for (in)equivalence using Hermitian version of Plesken-Souvignier algorithm
- Siegel-type mass formula tells you when to stop

$\mathfrak{p}$-neighbours and Hecke operators

$$\begin{aligned} L(x_i)_{\mathfrak{p}} &= \left(\bar{\mathfrak{p}}\mathfrak{p}^{-1} v_1 \oplus \mathcal{O}_K v_2 \oplus \cdots \oplus \mathcal{O}_K v_{n-1} \oplus \mathcal{O}_K v_n\right)_{\mathfrak{p}} \\ &= p^{-1}\mathbb{Z}_p v_1 \oplus \cdots \mathbb{Z}_p v_{n-1} \oplus \mathbb{Z}_p v_n. \end{aligned}$$

$$\begin{aligned} L(x_i)_{\bar{\mathfrak{p}}} &= \left(\bar{\mathfrak{p}}\mathfrak{p}^{-1} v_1 \oplus \mathcal{O}_K v_2 \oplus \cdots \oplus \mathcal{O}_K v_{n-1} \oplus \mathcal{O}_K v_n\right)_{\bar{\mathfrak{p}}} \\ &= p\mathbb{Z}_p v_1 \oplus \cdots \mathbb{Z}_p v_{n-1} \oplus \mathbb{Z}_p v_n. \end{aligned}$$

If $\varpi = \mathrm{diag}(p, 1, \ldots, 1) \in \mathrm{GL}_n(\mathbb{Q}_p)^2 = G(\mathbb{Q}_p) \hookrightarrow G(\mathbb{A}_f)$ and $L = g \cdot L_0$, $g \in G(\mathbb{A}_f)$, then

$$\{L(x_i)\} \longleftrightarrow Kg(\varpi, {}^t\varpi^{-1})K/K.$$

It follows that

$$(f | T(\varpi, {}^t\varpi^{-1}))(L) = \sum_{L \overset{\mathfrak{p}}{\rightsquigarrow} L'} f(L')$$

A slight generalization

- Suppose $X \subset \bar{\mathfrak{p}}L - pL$ is such that $\bar{X}$ is a $(k-1)$-plane in $\mathbb{P}(\bar{\mathfrak{p}}L/pL)$, $1 \le k \le n-1$.
- We can define a $(\mathfrak{p}, k)$-neighbour $L(X)$ of L such that

$$\{L(X)\} \longleftrightarrow Kg(\varpi, {}^t\varpi^{-1})K/K,$$

where $L = g \cdot L_0$ and $\varpi = (\underbrace{p, \dots, p}_{k}, \underbrace{0, \dots, 0}_{n-k})$.

- We have:

$$(f|T(\varpi, {}^t\varpi^{-1}))(L) = \sum_{L \overset{\mathfrak{p}}{\rightsquigarrow} L'} f(L').$$

To-do list/questions

- Write more code!
- How do you compute Hecke operators at nonsplit primes? (Need to understand Bruhat-Tits theory.)
- Iwahori level structure at some prime? Higher level structure?
- Adapt to to other groups where the Bruhat-Tits buildings can be described in terms of lattice chains. Exceptional lie groups?
- algorithms for testing hermitian and quaternionic lattices for equivalence