Computing classical modular forms as orthogonal modular forms

John Voight
Dartmouth College

joint work with
Jeffery Hein and Gonzalo Tornaría

AGC^{2}T-17
CIRM, Luminy
21 June 2017

Birch's ternary method

Birch's ternary method

In 1991 (based on a 1988 talk in Luminy), Birch gave an algorithm to compute classical modular forms of weight 2 based on the Hecke action on classes of ternary quadratic forms.

Birch's ternary method

In 1991 (based on a 1988 talk in Luminy), Birch gave an algorithm to compute classical modular forms of weight 2 based on the Hecke action on classes of ternary quadratic forms.

Birch begins by analogy with *la méthode des graphes* due to Mestre–Oesterlé:

Birch's ternary method

In 1991 (based on a 1988 talk in Luminy), Birch gave an algorithm to compute classical modular forms of weight 2 based on the Hecke action on classes of ternary quadratic forms.

Birch begins by analogy with *la méthode des graphes* due to Mestre–Oesterlé: there is a natural Hecke action on the set of supersingular elliptic curves in prime characteristic N via the p-isogeny graph, and this Hecke module is isomorphic to $M_2(\Gamma_0(N))$.

Birch's ternary method

In 1991 (based on a 1988 talk in Luminy), Birch gave an algorithm to compute classical modular forms of weight 2 based on the Hecke action on classes of ternary quadratic forms.

Birch begins by analogy with *la méthode des graphes* due to Mestre–Oesterlé: there is a natural Hecke action on the set of supersingular elliptic curves in prime characteristic N via the p-isogeny graph, and this Hecke module is isomorphic to $M_2(\Gamma_0(N))$.

Birch sought a method that would work more generally for composite N.

Birch's ternary method

Birch's ternary method

Birch says:

> *[T]here is a great deal of interesting information to be calculated; since the program is very fast, it is possible for anyone who owns it to generate interesting numbers much faster than it is possible to read them. ... [However,] this attempt ... has so far failed in two ways: first, it usually gives only half the information needed, and, second, when the level is not square-free it gives even less information. At least the program is very fast!*

Birch's ternary method

Birch says:

> *[T]here is a great deal of interesting information to be calculated; since the program is very fast, it is possible for anyone who owns it to generate interesting numbers much faster than it is possible to read them. ... [However,] this attempt ... has so far failed in two ways: first, it usually gives only half the information needed, and, second, when the level is not square-free it gives even less information. At least the program is very fast!*

In this talk, we will show how to extend Birch's method to compute forms of *nonsquare* level N.

Birch's ternary method

Birch says:

> *[T]here is a great deal of interesting information to be calculated; since the program is very fast, it is possible for anyone who owns it to generate interesting numbers much faster than it is possible to read them. ... [However,] this attempt ... has so far failed in two ways: first, it usually gives only half the information needed, and, second, when the level is not square-free it gives even less information. At least the program is very fast!*

In this talk, we will show how to extend Birch's method to compute forms of *nonsquare* level N. It is indeed very fast!

Birch's ternary method

Birch says:

> *[T]here is a great deal of interesting information to be calculated; since the program is very fast, it is possible for anyone who owns it to generate interesting numbers much faster than it is possible to read them. ... [However,] this attempt ... has so far failed in two ways: first, it usually gives only half the information needed, and, second, when the level is not square-free it gives even less information. At least the program is very fast!*

In this talk, we will show how to extend Birch's method to compute forms of *nonsquare* level N. It is indeed very fast!

Our method works for Hilbert modular forms (over totally real fields), but we'll mostly stick to $\mathbb{Q}$ in the talk.

Quadratic forms and lattices

Quadratic forms and lattices

Let $Q : V \to \mathbb{Q}$ be a positive definite ternary ($\dim_{\mathbb{Q}} V = 3$) quadratic space

Quadratic forms and lattices

Let $Q : V \to \mathbb{Q}$ be a positive definite ternary ($\dim_{\mathbb{Q}} V = 3$) quadratic space with associated bilinear form

$$T(x, y) := Q(x + y) - Q(x) - Q(y) \quad \text{for } x, y \in V.$$

Quadratic forms and lattices

Let $Q : V \to \mathbb{Q}$ be a positive definite ternary ($\dim_{\mathbb{Q}} V = 3$) quadratic space with associated bilinear form

$$T(x, y) := Q(x + y) - Q(x) - Q(y) \quad \text{for } x, y \in V.$$

Let $\Lambda < V$ be a lattice ($\Lambda \simeq \mathbb{Z}^3$) that is **integral**, so $Q(\Lambda) \subseteq \mathbb{Z}$.

Quadratic forms and lattices

Let $Q : V \to \mathbb{Q}$ be a positive definite ternary ($\dim_{\mathbb{Q}} V = 3$) quadratic space with associated bilinear form

$$T(x, y) := Q(x + y) - Q(x) - Q(y) \quad \text{for } x, y \in V.$$

Let $\Lambda < V$ be a lattice ($\Lambda \simeq \mathbb{Z}^3$) that is **integral**, so $Q(\Lambda) \subseteq \mathbb{Z}$. Choosing a basis $\Lambda = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \simeq \mathbb{Z}^3$

Quadratic forms and lattices

Let $Q : V \to \mathbb{Q}$ be a positive definite ternary ($\dim_{\mathbb{Q}} V = 3$) quadratic space with associated bilinear form

$$T(x, y) := Q(x + y) - Q(x) - Q(y) \quad \text{for } x, y \in V.$$

Let $\Lambda < V$ be a lattice ($\Lambda \simeq \mathbb{Z}^3$) that is **integral**, so $Q(\Lambda) \subseteq \mathbb{Z}$.
Choosing a basis $\Lambda = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \simeq \mathbb{Z}^3$ gives a quadratic form

$$Q_\Lambda(xe_1 + ye_2 + ze_3) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x, y, z]$$

Quadratic forms and lattices

Let $Q : V \to \mathbb{Q}$ be a positive definite ternary ($\dim_{\mathbb{Q}} V = 3$) quadratic space with associated bilinear form

$$T(x, y) := Q(x + y) - Q(x) - Q(y) \quad \text{for } x, y \in V.$$

Let $\Lambda < V$ be a lattice ($\Lambda \simeq \mathbb{Z}^3$) that is **integral**, so $Q(\Lambda) \subseteq \mathbb{Z}$. Choosing a basis $\Lambda = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \simeq \mathbb{Z}^3$ gives a quadratic form

$$Q_\Lambda(xe_1 + ye_2 + ze_3) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x, y, z]$$

and vice versa.

Quadratic forms and lattices

Let $Q : V \to \mathbb{Q}$ be a positive definite ternary ($\dim_{\mathbb{Q}} V = 3$) quadratic space with associated bilinear form

$$T(x, y) := Q(x + y) - Q(x) - Q(y) \quad \text{for } x, y \in V.$$

Let $\Lambda < V$ be a lattice ($\Lambda \simeq \mathbb{Z}^3$) that is **integral**, so $Q(\Lambda) \subseteq \mathbb{Z}$. Choosing a basis $\Lambda = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \simeq \mathbb{Z}^3$ gives a quadratic form

$$Q_\Lambda(xe_1 + ye_2 + ze_3) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x, y, z]$$

and vice versa.

Define

$$\operatorname{disc}(\Lambda) = \operatorname{disc}(Q_\Lambda) := \det(T(e_i, e_j))_{i,j}/2 = \frac{1}{2} \det \begin{pmatrix} 2a & w & v \\ w & 2b & u \\ v & u & 2c \end{pmatrix}$$

Quadratic forms and lattices

Let $Q : V \to \mathbb{Q}$ be a positive definite ternary ($\dim_{\mathbb{Q}} V = 3$) quadratic space with associated bilinear form

$$T(x,y) := Q(x+y) - Q(x) - Q(y) \quad \text{for } x, y \in V.$$

Let $\Lambda < V$ be a lattice ($\Lambda \simeq \mathbb{Z}^3$) that is **integral**, so $Q(\Lambda) \subseteq \mathbb{Z}$. Choosing a basis $\Lambda = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \simeq \mathbb{Z}^3$ gives a quadratic form

$$Q_\Lambda(xe_1 + ye_2 + ze_3) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x,y,z]$$

and vice versa.

Define

$$\begin{aligned}\operatorname{disc}(\Lambda) = \operatorname{disc}(Q_\Lambda) := \det(T(e_i,e_j))_{i,j}/2 &= \frac{1}{2}\det\begin{pmatrix} 2a & w & v \\ w & 2b & u \\ v & u & 2c \end{pmatrix} \\ &= 4abc + uvw - au^2 - bv^2 - cw^2 \in \mathbb{Z}_{>0}\end{aligned}$$

Isometries and genus

Isometries and genus

Let

$$\mathrm{O}(V) := \{g \in \mathrm{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\}$$

Isometries and genus

Let

$$\begin{aligned}
\mathrm{O}(V) &:= \{g \in \mathrm{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\} \\
\mathrm{SO}(V) &:= \mathrm{O}(V) \cap \mathrm{SL}(V)
\end{aligned}$$

Isometries and genus

Let

$$\begin{aligned} \mathrm{O}(V) &:= \{g \in \mathrm{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\} \\ \mathrm{SO}(V) &:= \mathrm{O}(V) \cap \mathrm{SL}(V) \end{aligned}$$

Define $O(\Lambda)$ etc. similarly;

Isometries and genus

Let

$$\mathrm{O}(V) := \{g \in \mathrm{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\}$$
$$\mathrm{SO}(V) := \mathrm{O}(V) \cap \mathrm{SL}(V)$$

Define $O(\Lambda)$ etc. similarly; we have $\#O(\Lambda) < \infty$.

Isometries and genus

Let

$$\begin{aligned} \mathrm{O}(V) &:= \{g \in \mathrm{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\} \\ \mathrm{SO}(V) &:= \mathrm{O}(V) \cap \mathrm{SL}(V) \end{aligned}$$

Define $O(\Lambda)$ etc. similarly; we have $\#O(\Lambda) < \infty$.

Lattices $\Lambda, \Pi \subset V$ are **isometric**,

Isometries and genus

Let

$$\begin{aligned} \mathrm{O}(V) &:= \{g \in \mathrm{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\} \\ \mathrm{SO}(V) &:= \mathrm{O}(V) \cap \mathrm{SL}(V) \end{aligned}$$

Define $O(\Lambda)$ etc. similarly; we have $\#O(\Lambda) < \infty$.

Lattices $\Lambda, \Pi \subset V$ are **isometric**, written $\Lambda \simeq \Pi$,

Isometries and genus

Let

$$\begin{aligned} \mathrm{O}(V) &:= \{g \in \mathrm{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\} \\ \mathrm{SO}(V) &:= \mathrm{O}(V) \cap \mathrm{SL}(V) \end{aligned}$$

Define $O(\Lambda)$ etc. similarly; we have $\#O(\Lambda) < \infty$.

Lattices $\Lambda, \Pi \subset V$ are **isometric**, written $\Lambda \simeq \Pi$, if there exists $g \in \mathrm{O}(V)$ such that $g\Lambda = \Pi$. Same with isometric over $\mathbb{Q}_p$.

Isometries and genus

Let

$$\begin{aligned} \mathrm{O}(V) &:= \{g \in \mathrm{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\} \\ \mathrm{SO}(V) &:= \mathrm{O}(V) \cap \mathrm{SL}(V) \end{aligned}$$

Define $O(\Lambda)$ etc. similarly; we have $\#O(\Lambda) < \infty$.

Lattices $\Lambda, \Pi \subset V$ are **isometric**, written $\Lambda \simeq \Pi$, if there exists $g \in \mathrm{O}(V)$ such that $g\Lambda = \Pi$. Same with isometric over $\mathbb{Q}_p$.

The **genus** of Λ is

$$\mathrm{Gen}(\Lambda) := \{\Pi < V : \Lambda_p \simeq \Pi_p \text{ for all } p\}.$$

Isometries and genus

Let

$$\begin{aligned} \mathrm{O}(V) &:= \{g \in \mathrm{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\} \\ \mathrm{SO}(V) &:= \mathrm{O}(V) \cap \mathrm{SL}(V) \end{aligned}$$

Define $O(\Lambda)$ etc. similarly; we have $\#O(\Lambda) < \infty$.

Lattices $\Lambda, \Pi \subset V$ are **isometric**, written $\Lambda \simeq \Pi$, if there exists $g \in \mathrm{O}(V)$ such that $g\Lambda = \Pi$. Same with isometric over $\mathbb{Q}_p$.

The **genus** of Λ is

$$\mathrm{Gen}(\Lambda) := \{\Pi < V : \Lambda_p \simeq \Pi_p \text{ for all } p\}.$$

The **class set** $\mathrm{Cl}(\Lambda)$ is the set of isometry classes in $\mathrm{Gen}(\Lambda)$.

Isometries and genus

Let

$$\begin{aligned} \mathrm{O}(V) &:= \{g \in \mathrm{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\} \\ \mathrm{SO}(V) &:= \mathrm{O}(V) \cap \mathrm{SL}(V) \end{aligned}$$

Define $O(\Lambda)$ etc. similarly; we have $\#O(\Lambda) < \infty$.

Lattices $\Lambda, \Pi \subset V$ are **isometric**, written $\Lambda \simeq \Pi$, if there exists $g \in \mathrm{O}(V)$ such that $g\Lambda = \Pi$. Same with isometric over $\mathbb{Q}_p$.

The **genus** of Λ is

$$\mathrm{Gen}(\Lambda) := \{\Pi < V : \Lambda_p \simeq \Pi_p \text{ for all } p\}.$$

The **class set** $\mathrm{Cl}(\Lambda)$ is the set of isometry classes in $\mathrm{Gen}(\Lambda)$.

By the geometry of numbers, $\#\,\mathrm{Cl}(\Lambda) < \infty$.

Neighbors

Neighbors

Kneser's theory of p-neighbors gives an effective method to compute the class set;

Neighbors

Kneser's theory of p-neighbors gives an effective method to compute the class set; it also gives the Hecke action!

Neighbors

Kneser's theory of p-neighbors gives an effective method to compute the class set; it also gives the Hecke action!

Let $p \nmid \operatorname{disc}(\Lambda)$ be prime (still with Λ integral); $p = 2$ is OK.

Neighbors

Kneser's theory of p-neighbors gives an effective method to compute the class set; it also gives the Hecke action!

Let $p \nmid \operatorname{disc}(\Lambda)$ be prime (still with Λ integral); $p = 2$ is OK.

We say that a lattice $\Pi < V$ is a p-**neighbor** of Λ,

Neighbors

Kneser's theory of p-neighbors gives an effective method to compute the class set; it also gives the Hecke action!

Let $p \nmid \operatorname{disc}(\Lambda)$ be prime (still with Λ integral); $p = 2$ is OK.

We say that a lattice $\Pi < V$ is a p-**neighbor** of Λ, and write $\Pi \sim_p \Lambda$,

Neighbors

Kneser's theory of p-neighbors gives an effective method to compute the class set; it also gives the Hecke action!

Let $p \nmid \mathrm{disc}(\Lambda)$ be prime (still with Λ integral); $p = 2$ is OK.

We say that a lattice $\Pi < V$ is a p-**neighbor** of Λ, and write $\Pi \sim_p \Lambda$, if

$$[\Lambda : \Lambda \cap \Pi] = [\Pi : \Lambda \cap \Pi] = p.$$

Neighbors

Kneser's theory of p-neighbors gives an effective method to compute the class set; it also gives the Hecke action!

Let $p \nmid \operatorname{disc}(\Lambda)$ be prime (still with Λ integral); $p = 2$ is OK.

We say that a lattice $\Pi < V$ is a p-**neighbor** of Λ, and write $\Pi \sim_p \Lambda$, if

$$[\Lambda : \Lambda \cap \Pi] = [\Pi : \Lambda \cap \Pi] = p.$$

If $\Lambda \sim_p \Pi$, then:

- $\operatorname{disc}(\Lambda) = \operatorname{disc}(\Pi)$,
- Π is integral, and
- $\Pi \in \operatorname{Gen}(\Lambda)$.

Neighbors

Kneser's theory of p-neighbors gives an effective method to compute the class set; it also gives the Hecke action!

Let $p \nmid \operatorname{disc}(\Lambda)$ be prime (still with Λ integral); $p = 2$ is OK.

We say that a lattice $\Pi < V$ is a p-**neighbor** of Λ, and write $\Pi \sim_p \Lambda$, if

$$[\Lambda : \Lambda \cap \Pi] = [\Pi : \Lambda \cap \Pi] = p.$$

If $\Lambda \sim_p \Pi$, then:

- $\operatorname{disc}(\Lambda) = \operatorname{disc}(\Pi)$,
- Π is integral, and
- $\Pi \in \operatorname{Gen}(\Lambda)$.

Moreover, there is an effectively computable finite set S of primes such that every $[\Lambda'] \in \operatorname{Cl}(\Lambda)$ is an **iterated** S-**neighbor**

Neighbors

Kneser's theory of p-neighbors gives an effective method to compute the class set; it also gives the Hecke action!

Let $p \nmid \operatorname{disc}(\Lambda)$ be prime (still with Λ integral); $p = 2$ is OK.

We say that a lattice $\Pi < V$ is a p-**neighbor** of Λ, and write $\Pi \sim_p \Lambda$, if

$$[\Lambda : \Lambda \cap \Pi] = [\Pi : \Lambda \cap \Pi] = p.$$

If $\Lambda \sim_p \Pi$, then:

- $\operatorname{disc}(\Lambda) = \operatorname{disc}(\Pi)$,
- Π is integral, and
- $\Pi \in \operatorname{Gen}(\Lambda)$.

Moreover, there is an effectively computable finite set S of primes such that every $[\Lambda'] \in \operatorname{Cl}(\Lambda)$ is an **iterated** S-**neighbor**

$$\Lambda \sim_{p_1} \Lambda_1 \sim_{p_2} \cdots \sim_{p_r} \Lambda_r \simeq \Lambda'$$

with $p_i \in S$.

Neighbors

Kneser's theory of p-neighbors gives an effective method to compute the class set; it also gives the Hecke action!

Let $p \nmid \operatorname{disc}(\Lambda)$ be prime (still with Λ integral); $p = 2$ is OK.

We say that a lattice $\Pi < V$ is a p-**neighbor** of Λ, and write $\Pi \sim_p \Lambda$, if

$$[\Lambda : \Lambda \cap \Pi] = [\Pi : \Lambda \cap \Pi] = p.$$

If $\Lambda \sim_p \Pi$, then:

- $\operatorname{disc}(\Lambda) = \operatorname{disc}(\Pi)$,
- Π is integral, and
- $\Pi \in \operatorname{Gen}(\Lambda)$.

Moreover, there is an effectively computable finite set S of primes such that every $[\Lambda'] \in \operatorname{Cl}(\Lambda)$ is an **iterated** S-**neighbor**

$$\Lambda \sim_{p_1} \Lambda_1 \sim_{p_2} \cdots \sim_{p_r} \Lambda_r \simeq \Lambda'$$

with $p_i \in S$. Typically we may take $S = \{p\}$ for any $p \nmid \operatorname{disc}(\Lambda)$.

Explicit neighbors

Explicit neighbors

The set of p-neighbors is efficiently computable, as follows.

Explicit neighbors

The set of p-neighbors is efficiently computable, as follows.

- $\Pi \sim_p \Lambda$ if and only if

Explicit neighbors

The set of p-neighbors is efficiently computable, as follows.

- $\Pi \sim_p \Lambda$ if and only if $\Lambda_q = \Pi_q$ for all $q \neq p$, and

Explicit neighbors

The set of p-neighbors is efficiently computable, as follows.

- $\Pi \sim_p \Lambda$ if and only if $\Lambda_q = \Pi_q$ for all $q \neq p$, and there exists a $\mathbb{Z}_p$-basis e_1, e_2, e_3 for Λ_p (called a p-**standard basis**) such that

Explicit neighbors

The set of p-neighbors is efficiently computable, as follows.

- $\Pi \sim_p \Lambda$ if and only if $\Lambda_q = \Pi_q$ for all $q \neq p$, and there exists a $\mathbb{Z}_p$-basis e_1, e_2, e_3 for Λ_p (called a p-**standard basis**) such that

$$\Lambda_p = \mathbb{Z}_p e_1 + \mathbb{Z}_p e_2 + \mathbb{Z}_p e_3$$
$$\Pi_p = \mathbb{Z}_p(\tfrac{1}{p} e_1) + \mathbb{Z}_p(p e_2) + \mathbb{Z}_p e_3$$

and $Q(xe_1 + ye_2 + ze_3) = xy + Q(e_3)z^2$.

Explicit neighbors

The set of p-neighbors is efficiently computable, as follows.

- $\Pi \sim_p \Lambda$ if and only if $\Lambda_q = \Pi_q$ for all $q \neq p$, and there exists a $\mathbb{Z}_p$-basis e_1, e_2, e_3 for Λ_p (called a p-**standard basis**) such that

$$\begin{aligned} \Lambda_p &= \mathbb{Z}_p e_1 + \mathbb{Z}_p e_2 + \mathbb{Z}_p e_3 \\ \Pi_p &= \mathbb{Z}_p(\tfrac{1}{p} e_1) + \mathbb{Z}_p(p e_2) + \mathbb{Z}_p e_3 \end{aligned}$$

  and $Q(xe_1 + ye_2 + ze_3) = xy + Q(e_3)z^2$.
- $\Pi \sim_p \Lambda$ if and only if there exists $v \in \Lambda$ such that $Q(v) \equiv 0 \pmod{2p^2}$ and

$$\Pi = p^{-1}v + \{w \in \Lambda : T(v, w) \in p\mathbb{Z}\}.$$

Explicit neighbors

The set of p-neighbors is efficiently computable, as follows.

- $\Pi \sim_p \Lambda$ if and only if $\Lambda_q = \Pi_q$ for all $q \neq p$, and there exists a $\mathbb{Z}_p$-basis e_1, e_2, e_3 for Λ_p (called a p-**standard basis**) such that

$$\Lambda_p = \mathbb{Z}_p e_1 + \mathbb{Z}_p e_2 + \mathbb{Z}_p e_3$$
$$\Pi_p = \mathbb{Z}_p(\tfrac{1}{p} e_1) + \mathbb{Z}_p(p e_2) + \mathbb{Z}_p e_3$$

  and $Q(xe_1 + ye_2 + ze_3) = xy + Q(e_3)z^2$.
- $\Pi \sim_p \Lambda$ if and only if there exists $v \in \Lambda$ such that $Q(v) \equiv 0 \pmod{2p^2}$ and

$$\Pi = p^{-1}v + \{w \in \Lambda : T(v, w) \in p\mathbb{Z}\}.$$

  The line spanned by v uniquely determines Π,

Explicit neighbors

The set of p-neighbors is efficiently computable, as follows.

- $\Pi \sim_p \Lambda$ if and only if $\Lambda_q = \Pi_q$ for all $q \neq p$, and there exists a $\mathbb{Z}_p$-basis e_1, e_2, e_3 for Λ_p (called a p-**standard basis**) such that

$$\Lambda_p = \mathbb{Z}_p e_1 + \mathbb{Z}_p e_2 + \mathbb{Z}_p e_3$$
$$\Pi_p = \mathbb{Z}_p(\tfrac{1}{p} e_1) + \mathbb{Z}_p(p e_2) + \mathbb{Z}_p e_3$$

  and $Q(xe_1 + ye_2 + ze_3) = xy + Q(e_3)z^2$.
- $\Pi \sim_p \Lambda$ if and only if there exists $v \in \Lambda$ such that $Q(v) \equiv 0 \pmod{2p^2}$ and

$$\Pi = p^{-1}v + \{w \in \Lambda : T(v, w) \in p\mathbb{Z}\}.$$

  The line spanned by v uniquely determines Π, accordingly there are exactly $p + 1$ neighbors Π.

Example

Example

Let $\Lambda = \mathbb{Z}^3 = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \subset \mathbb{Q}^3$ have the quadratic form

$$Q_\Lambda(x, y, z) = x^2 + y^2 + 3z^2 + xz$$

Example

Let $\Lambda = \mathbb{Z}^3 = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \subset \mathbb{Q}^3$ have the quadratic form

$$Q_\Lambda(x, y, z) = x^2 + y^2 + 3z^2 + xz$$

and bilinear form given by

$$[T_\Lambda] = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 6 \end{pmatrix}.$$

Example

Let $\Lambda = \mathbb{Z}^3 = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \subset \mathbb{Q}^3$ have the quadratic form

$$Q_\Lambda(x, y, z) = x^2 + y^2 + 3z^2 + xz$$

and bilinear form given by

$$[T_\Lambda] = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 6 \end{pmatrix}.$$

Thus

$$\mathrm{disc}(Q_\Lambda) = 11.$$

Example

Let $\Lambda = \mathbb{Z}^3 = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \subset \mathbb{Q}^3$ have the quadratic form

$$Q_\Lambda(x, y, z) = x^2 + y^2 + 3z^2 + xz$$

and bilinear form given by

$$[T_\Lambda] = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 6 \end{pmatrix}.$$

Thus

$$\operatorname{disc}(Q_\Lambda) = 11.$$

We have $\# \operatorname{Cl}(\Lambda) = 2$, with the nontrivial class represented by the 3-neighbor

$$\Lambda' = \mathbb{Z}e_1 + 3\mathbb{Z}e_2 + \tfrac{1}{3}\mathbb{Z}(e_1 + 2e_2 + e_3)$$

Example

Let $\Lambda = \mathbb{Z}^3 = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \subset \mathbb{Q}^3$ have the quadratic form

$$Q_\Lambda(x, y, z) = x^2 + y^2 + 3z^2 + xz$$

and bilinear form given by

$$[T_\Lambda] = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 6 \end{pmatrix}.$$

Thus

$$\operatorname{disc}(Q_\Lambda) = 11.$$

We have $\# \operatorname{Cl}(\Lambda) = 2$, with the nontrivial class represented by the 3-neighbor

$$\Lambda' = \mathbb{Z}e_1 + 3\mathbb{Z}e_2 + \tfrac{1}{3}\mathbb{Z}(e_1 + 2e_2 + e_3)$$

with corresponding quadratic form

$$Q_{\Lambda'}(x, y, z) = x^2 + 9y^2 + z^2 + 4yz + xz.$$

Hecke action

Hecke action

The space of **orthogonal modular forms for** Λ (with trivial weight) is

$$M(\mathrm{O}(\Lambda)) := \mathrm{Map}(\mathrm{Cl}(\Lambda), \mathbb{C}).$$

Hecke action

The space of **orthogonal modular forms for** Λ (with trivial weight) is

$$M(\mathrm{O}(\Lambda)) := \mathrm{Map}(\mathrm{Cl}(\Lambda), \mathbb{C}).$$

In the basis of characteristic functions for Λ we have $M(\mathrm{O}(\Lambda)) \simeq \mathbb{C}^h$ where $h = \#\,\mathrm{Cl}(\Lambda)$.

Hecke action

The space of **orthogonal modular forms for** Λ (with trivial weight) is

$$M(\mathrm{O}(\Lambda)) := \mathrm{Map}(\mathrm{Cl}(\Lambda), \mathbb{C}).$$

In the basis of characteristic functions for Λ we have $M(\mathrm{O}(\Lambda)) \simeq \mathbb{C}^h$ where $h = \#\,\mathrm{Cl}(\Lambda)$.

For $p \nmid \mathrm{disc}(\Lambda)$, define the **Hecke operator**

$$\begin{aligned} T_p : M(\mathrm{O}(\Lambda)) &\to M(\mathrm{O}(\Lambda)) \\ f &\mapsto T_p(f) \end{aligned}$$

Hecke action

The space of **orthogonal modular forms for** Λ (with trivial weight) is

$$M(\mathrm{O}(\Lambda)) := \mathrm{Map}(\mathrm{Cl}(\Lambda), \mathbb{C}).$$

In the basis of characteristic functions for Λ we have $M(\mathrm{O}(\Lambda)) \simeq \mathbb{C}^h$ where $h = \#\,\mathrm{Cl}(\Lambda)$.

For $p \nmid \mathrm{disc}(\Lambda)$, define the **Hecke operator**

$$\begin{aligned} T_p : M(\mathrm{O}(\Lambda)) &\to M(\mathrm{O}(\Lambda)) \\ f &\mapsto T_p(f) \end{aligned}$$

$$T_p(f)([\Lambda'])$$

Hecke action

The space of **orthogonal modular forms for** Λ (with trivial weight) is

$$M(\mathrm{O}(\Lambda)) := \mathrm{Map}(\mathrm{Cl}(\Lambda), \mathbb{C}).$$

In the basis of characteristic functions for Λ we have $M(\mathrm{O}(\Lambda)) \simeq \mathbb{C}^h$ where $h = \#\,\mathrm{Cl}(\Lambda)$.

For $p \nmid \mathrm{disc}(\Lambda)$, define the **Hecke operator**

$$\begin{aligned} T_p : M(\mathrm{O}(\Lambda)) &\to M(\mathrm{O}(\Lambda)) \\ f &\mapsto T_p(f) \\ T_p(f)([\Lambda']) &:= \sum_{\Pi' \sim_p \Lambda'} f([\Pi']). \end{aligned}$$

Hecke action

The space of **orthogonal modular forms for** Λ (with trivial weight) is

$$M(\mathrm{O}(\Lambda)) := \mathrm{Map}(\mathrm{Cl}(\Lambda), \mathbb{C}).$$

In the basis of characteristic functions for Λ we have $M(\mathrm{O}(\Lambda)) \simeq \mathbb{C}^h$ where $h = \#\,\mathrm{Cl}(\Lambda)$.

For $p \nmid \mathrm{disc}(\Lambda)$, define the **Hecke operator**

$$\begin{aligned} T_p : M(\mathrm{O}(\Lambda)) &\to M(\mathrm{O}(\Lambda)) \\ f &\mapsto T_p(f) \\ T_p(f)([\Lambda']) &:= \sum_{\Pi' \sim_p \Lambda'} f([\Pi']). \end{aligned}$$

The operators T_p commute and are self-adjoint with respect to a natural inner product, so there is a basis of simultaneous eigenvectors, called **eigenforms**.

Computing the Hecke action

Computing the Hecke action

To compute the matrix representing the Hecke operator, we need to sort p-neighbors of a lattice according to their isometry class.

Computing the Hecke action

To compute the matrix representing the Hecke operator, we need to sort p-neighbors of a lattice according to their isometry class.

This can be accomplished on lattices using an algorithm of Plesken–Souveignier:

Computing the Hecke action

To compute the matrix representing the Hecke operator, we need to sort p-neighbors of a lattice according to their isometry class.

This can be accomplished on lattices using an algorithm of Plesken–Souveignier: match up short vectors and use lots of tricks to compute an isometry or rule it out as early as possible.

Computing the Hecke action

To compute the matrix representing the Hecke operator, we need to sort p-neighbors of a lattice according to their isometry class.

This can be accomplished on lattices using an algorithm of Plesken–Souveignier: match up short vectors and use lots of tricks to compute an isometry or rule it out as early as possible. This is very fast in practice and (in fixed dimension) is also theoretically efficient.

Computing the Hecke action

To compute the matrix representing the Hecke operator, we need to sort p-neighbors of a lattice according to their isometry class.

This can be accomplished on lattices using an algorithm of Plesken–Souveignier: match up short vectors and use lots of tricks to compute an isometry or rule it out as early as possible. This is very fast in practice and (in fixed dimension) is also theoretically efficient.

One can do even better:

Computing the Hecke action

To compute the matrix representing the Hecke operator, we need to sort p-neighbors of a lattice according to their isometry class.

This can be accomplished on lattices using an algorithm of Plesken–Souveignier: match up short vectors and use lots of tricks to compute an isometry or rule it out as early as possible. This is very fast in practice and (in fixed dimension) is also theoretically efficient.

One can do even better: there is an explicit reduction theory of integral ternary quadratic forms due to Eisenstein which generalizes Gauss reduction of integral quadratic forms.

Computing the Hecke action

To compute the matrix representing the Hecke operator, we need to sort p-neighbors of a lattice according to their isometry class.

This can be accomplished on lattices using an algorithm of Plesken–Souveignier: match up short vectors and use lots of tricks to compute an isometry or rule it out as early as possible. This is very fast in practice and (in fixed dimension) is also theoretically efficient.

One can do even better: there is an explicit reduction theory of integral ternary quadratic forms due to Eisenstein which generalizes Gauss reduction of integral quadratic forms. The result is a unique reduced form so that isometry testing becomes table lookup.

Example

Example

In the running example with discriminant 11,

Example

In the running example with discriminant 11, we compute

$$[T_3] = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}, \quad [T_5] = \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}, \quad \ldots .$$

Example

In the running example with discriminant 11, we compute

$$[T_3] = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}, \quad [T_5] = \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}, \quad \dots .$$

The constant function $e = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in M(\mathrm{O}(\Lambda))$

Example

In the running example with discriminant 11, we compute

$$[T_3] = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}, \quad [T_5] = \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}, \quad \dots .$$

The constant function $e = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in M(\mathrm{O}(\Lambda))$ is an *Eisenstein series* with $T_p(e) = (p+1)e$.

Example

In the running example with discriminant 11, we compute

$$[T_3] = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}, \quad [T_5] = \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}, \quad \dots .$$

The constant function $e = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in M(\mathrm{O}(\Lambda))$ is an *Eisenstein series* with $T_p(e) = (p+1)e$.

Another eigenvector is $f = \begin{pmatrix} 2 \\ -3 \end{pmatrix}$ with $T_p(f) = a_p(f)$:

$$a_3 = -1, a_5 = 1, \dots, a_{11} = 1.$$

Example

In the running example with discriminant 11, we compute

$$[T_3] = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}, \quad [T_5] = \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}, \quad \ldots.$$

The constant function $e = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in M(\mathrm{O}(\Lambda))$ is an *Eisenstein series* with $T_p(e) = (p+1)e$.

Another eigenvector is $f = \begin{pmatrix} 2 \\ -3 \end{pmatrix}$ with $T_p(f) = a_p(f)$:

$$a_3 = -1, a_5 = 1, \ldots, a_{11} = 1.$$

We match it with the modular form

$$\sum_{n=1}^{\infty} a_n q^n = \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2 = q - 2q^2 - q^3 + \ldots \in S_2(\Gamma_0(11)).$$

Example

In the running example with discriminant 11, we compute

$$[T_3] = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}, \quad [T_5] = \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}, \quad \dots.$$

The constant function $e = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in M(\mathrm{O}(\Lambda))$ is an *Eisenstein series* with $T_p(e) = (p+1)e$.

Another eigenvector is $f = \begin{pmatrix} 2 \\ -3 \end{pmatrix}$ with $T_p(f) = a_p(f)$:

$$a_3 = -1, a_5 = 1, \dots, a_{11} = 1.$$

We match it with the modular form

$$\sum_{n=1}^{\infty} a_n q^n = \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2 = q - 2q^2 - q^3 + \dots \in S_2(\Gamma_0(11)).$$

The *Atkin–Lehner* involution $z \mapsto \dfrac{-1}{11z}$ acts on $f(z)\,\mathrm{d}z$ with eigenvalue $w_{11} = -a_{11} = -1$.

Classical modular forms

Classical modular forms

Let $S(\mathrm{O}(\Lambda)) \subset M(\mathrm{O}(\Lambda))$ be the orthogonal complement of the constant functions.

Classical modular forms

Let $S(\mathrm{O}(\Lambda)) \subset M(\mathrm{O}(\Lambda))$ be the orthogonal complement of the constant functions.

Theorem (Birch, Hein)

Classical modular forms

Let $S(\mathrm{O}(\Lambda)) \subset M(\mathrm{O}(\Lambda))$ be the orthogonal complement of the constant functions.

Theorem (Birch, Hein)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree.

Let $S(\mathrm{O}(\Lambda)) \subset M(\mathrm{O}(\Lambda))$ be the orthogonal complement of the constant functions.

Theorem (Birch, Hein)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree. Let $\epsilon_p \in \{\pm 1\}$ be the p-Witt invariant for $p \mid N$ and let $D = \prod_{p:\epsilon_p=-1} p$.

Let $S(\mathrm{O}(\Lambda)) \subset M(\mathrm{O}(\Lambda))$ be the orthogonal complement of the constant functions.

Theorem (Birch, Hein)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree. Let $\epsilon_p \in \{\pm 1\}$ be the p-Witt invariant for $p \mid N$ and let $D = \prod_{p:\epsilon_p=-1} p$. Then there is a Hecke-equivariant inclusion

Classical modular forms

Let $S(\mathrm{O}(\Lambda)) \subset M(\mathrm{O}(\Lambda))$ be the orthogonal complement of the constant functions.

Theorem (Birch, Hein)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree. Let $\epsilon_p \in \{\pm 1\}$ be the p-Witt invariant for $p \mid N$ and let $D = \prod_{p : \epsilon_p = -1} p$. Then there is a Hecke-equivariant inclusion

$$S(\mathrm{O}(\Lambda)) \hookrightarrow S_2(\Gamma_0(N))$$

Classical modular forms

Let $S(\mathrm{O}(\Lambda)) \subset M(\mathrm{O}(\Lambda))$ be the orthogonal complement of the constant functions.

Theorem (Birch, Hein)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree. Let $\epsilon_p \in \{\pm 1\}$ be the p-Witt invariant for $p \mid N$ and let $D = \prod_{p : \epsilon_p = -1} p$. Then there is a Hecke-equivariant inclusion

$$S(\mathrm{O}(\Lambda)) \hookrightarrow S_2(\Gamma_0(N))$$

whose image is $S_2(\Gamma_0(N); D\text{-new}; w = \epsilon)$

Let $S(\mathrm{O}(\Lambda)) \subset M(\mathrm{O}(\Lambda))$ be the orthogonal complement of the constant functions.

Theorem (Birch, Hein)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree. Let $\epsilon_p \in \{\pm 1\}$ be the p-Witt invariant for $p \mid N$ and let $D = \prod_{p : \epsilon_p = -1} p$. Then there is a Hecke-equivariant inclusion

$$S(\mathrm{O}(\Lambda)) \hookrightarrow S_2(\Gamma_0(N))$$

whose image is $S_2(\Gamma_0(N); D\text{-new}; w = \epsilon) :=$

$\{f \in S_2(\Gamma_0(N)) : f$ is new at all $p \mid D$ and $W_p f = \epsilon_p f$ for all $p \mid N\}$.

Classical modular forms

Let $S(\mathrm{O}(\Lambda)) \subset M(\mathrm{O}(\Lambda))$ be the orthogonal complement of the constant functions.

Theorem (Birch, Hein)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree. Let $\epsilon_p \in \{\pm 1\}$ be the p-Witt invariant for $p \mid N$ and let $D = \prod_{p:\epsilon_p=-1} p$. Then there is a Hecke-equivariant inclusion

$$S(\mathrm{O}(\Lambda)) \hookrightarrow S_2(\Gamma_0(N))$$

whose image is $S_2(\Gamma_0(N); D\text{-new}; w = \epsilon) :=$

$\{f \in S_2(\Gamma_0(N)) : f \text{ is new at all } p \mid D \text{ and } W_p f = \epsilon_p f \text{ for all } p \mid N\}.$

Birch sketches two arguments for this theorem.

Classical modular forms

Let $S(\mathrm{O}(\Lambda)) \subset M(\mathrm{O}(\Lambda))$ be the orthogonal complement of the constant functions.

Theorem (Birch, Hein)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree. Let $\epsilon_p \in \{\pm 1\}$ be the p-Witt invariant for $p \mid N$ and let $D = \prod_{p:\epsilon_p=-1} p$. Then there is a Hecke-equivariant inclusion

$$S(\mathrm{O}(\Lambda)) \hookrightarrow S_2(\Gamma_0(N))$$

whose image is $S_2(\Gamma_0(N); D\text{-new}; w = \epsilon) :=$

$$\{f \in S_2(\Gamma_0(N)) : f \text{ is new at all } p \mid D \text{ and } W_p f = \epsilon_p f \text{ for all } p \mid N\}.$$

Birch sketches two arguments for this theorem. Hein gives a complete proof using one of these arguments, as follows.

Even Clifford algebra

Even Clifford algebra

Given

$$Q(x,y,z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x,y,z]$$

of discriminant $\operatorname{disc}(Q) = N$,

Even Clifford algebra

Given

$$Q(x, y, z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x, y, z]$$

of discriminant $\operatorname{disc}(Q) = N$, its **even Clifford algebra**

Even Clifford algebra

Given

$$Q(x, y, z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x, y, z]$$

of discriminant $\operatorname{disc}(Q) = N$, its **even Clifford algebra** is

$$\mathcal{O} = \mathrm{Clf}^0(Q)$$

Even Clifford algebra

Given

$$Q(x,y,z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x,y,z]$$

of discriminant $\operatorname{disc}(Q) = N$, its **even Clifford algebra** is

$$O = \mathrm{Clf}^0(Q) := \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

Even Clifford algebra

Given

$$Q(x,y,z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x,y,z]$$

of discriminant $\mathrm{disc}(Q) = N$, its **even Clifford algebra** is

$$O = \mathrm{Clf}^0(Q) := \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

with standard involution and multiplication laws

$$i^2 = ui - bc$$

Even Clifford algebra

Given

$$Q(x, y, z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x, y, z]$$

of discriminant $\operatorname{disc}(Q) = N$, its **even Clifford algebra** is

$$O = \operatorname{Clf}^0(Q) := \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

with standard involution and multiplication laws

$$i^2 = ui - bc \qquad\qquad jk = a\bar{i} = a(u - i)$$

Even Clifford algebra

Given

$$Q(x,y,z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x,y,z]$$

of discriminant $\operatorname{disc}(Q) = N$, its **even Clifford algebra** is

$$O = \mathrm{Clf}^0(Q) := \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

with standard involution and multiplication laws

$$\begin{aligned} i^2 &= ui - bc & \qquad jk &= a\bar{i} = a(u-i) \\ j^2 &= vj - ac & \qquad ki &= b\bar{j} = b(v-j) \\ k^2 &= wk - ab & \qquad ij &= c\bar{k} = c(w-k) \end{aligned}$$

Even Clifford algebra

Given

$$Q(x,y,z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x,y,z]$$

of discriminant $\operatorname{disc}(Q) = N$, its **even Clifford algebra** is

$$O = \mathrm{Clf}^0(Q) := \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

with standard involution and multiplication laws

$$\begin{aligned} i^2 &= ui - bc & \qquad jk &= a\bar{i} = a(u-i) \\ j^2 &= vj - ac & \qquad ki &= b\bar{j} = b(v-j) \\ k^2 &= wk - ab & \qquad ij &= c\bar{k} = c(w-k) \end{aligned}$$

so that e.g. $kj = \overline{\bar{j}\,\bar{k}} = -vw + ai + wj + vk$.

Even Clifford algebra

Given

$$Q(x,y,z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x,y,z]$$

of discriminant $\operatorname{disc}(Q) = N$, its **even Clifford algebra** is

$$O = \mathrm{Clf}^0(Q) := \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

with standard involution and multiplication laws

$$\begin{aligned} i^2 &= ui - bc & \qquad jk &= a\bar{i} = a(u-i) \\ j^2 &= vj - ac & \qquad ki &= b\bar{j} = b(v-j) \\ k^2 &= wk - ab & \qquad ij &= c\bar{k} = c(w-k) \end{aligned}$$

so that e.g. $kj = \overline{\bar{j}\,\bar{k}} = -vw + ai + wj + vk$.

Completing the square, we have

$$O \subset O \otimes \mathbb{Q} := B \simeq \left(\frac{w^2 - 4ab, -aN}{F}\right)$$

Even Clifford algebra

Given

$$Q(x,y,z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x,y,z]$$

of discriminant $\operatorname{disc}(Q) = N$, its **even Clifford algebra** is

$$O = \mathrm{Clf}^0(Q) := \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

with standard involution and multiplication laws

$$\begin{aligned} i^2 &= ui - bc & \qquad jk &= a\bar{i} = a(u-i) \\ j^2 &= vj - ac & \qquad ki &= b\bar{j} = b(v-j) \\ k^2 &= wk - ab & \qquad ij &= c\bar{k} = c(w-k) \end{aligned}$$

so that e.g. $kj = \overline{\bar{j}\,\bar{k}} = -vw + ai + wj + vk$.

Completing the square, we have

$$O \subset O \otimes \mathbb{Q} := B \simeq \left(\frac{w^2 - 4ab, -aN}{F}\right)$$

so O is an order in a definite quaternion algebra B.

Even Clifford algebra

Even Clifford algebra

The association $Q \mapsto O = \mathsf{Clf}^0(Q)$ is functorial

Even Clifford algebra

The association $Q \mapsto O = \mathsf{Clf}^0(Q)$ is functorial and induces a (reduced) discriminant-preserving bijection

Even Clifford algebra

The association $Q \mapsto O = \mathsf{Clf}^0(Q)$ is functorial and induces a (reduced) discriminant-preserving bijection

$$\left\{ \begin{array}{c} \text{Lattices } \Lambda \subset V \\ \text{up to isometry} \end{array} \right\}$$

Even Clifford algebra

The association $Q \mapsto O = \mathsf{Clf}^0(Q)$ is functorial and induces a (reduced) discriminant-preserving bijection

$$\left\{ \begin{array}{c} \text{Lattices } \Lambda \subset V \\ \text{up to isometry} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Quaternion orders } O \subset B \\ \text{up to isomorphism} \end{array} \right\}.$$

Even Clifford algebra

The association $Q \mapsto O = \mathrm{Clf}^0(Q)$ is functorial and induces a (reduced) discriminant-preserving bijection

$$\left\{ \begin{array}{c} \text{Lattices } \Lambda \subset V \\ \text{up to isometry} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Quaternion orders } O \subset B \\ \text{up to isomorphism} \end{array} \right\}.$$

Let $D = \mathrm{disc}(B) = \prod_{p \in \mathrm{Ram}(B)} p$.

Even Clifford algebra

The association $Q \mapsto O = \mathrm{Clf}^0(Q)$ is functorial and induces a (reduced) discriminant-preserving bijection

$$\left\{ \begin{array}{c} \text{Lattices } \Lambda \subset V \\ \text{up to isometry} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Quaternion orders } O \subset B \\ \text{up to isomorphism} \end{array} \right\}.$$

Let $D = \mathrm{disc}(B) = \prod_{p \in \mathrm{Ram}(B)} p$. If N is squarefree, then the p-Witt invariant is $w_p = -1$ if $p \mid D$ and $w_p = 1$ if $p \mid M = N/D$.

Even Clifford algebra

The association $Q \mapsto O = \mathrm{Clf}^0(Q)$ is functorial and induces a (reduced) discriminant-preserving bijection

$$\left\{ \begin{array}{c} \text{Lattices } \Lambda \subset V \\ \text{up to isometry} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Quaternion orders } O \subset B \\ \text{up to isomorphism} \end{array} \right\}.$$

Let $D = \mathrm{disc}(B) = \prod_{p \in \mathrm{Ram}(B)} p$. If N is squarefree, then the p-Witt invariant is $w_p = -1$ if $p \mid D$ and $w_p = 1$ if $p \mid M = N/D$.

We have an exact sequence

$$1 \to \mathbb{Q}^\times \to B^\times \to \mathrm{SO}(V) \to 1$$

Even Clifford algebra

The association $Q \mapsto O = \mathrm{Clf}^0(Q)$ is functorial and induces a (reduced) discriminant-preserving bijection

$$\left\{ \begin{array}{c} \text{Lattices } \Lambda \subset V \\ \text{up to isometry} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Quaternion orders } O \subset B \\ \text{up to isomorphism} \end{array} \right\}.$$

Let $D = \mathrm{disc}(B) = \prod_{p \in \mathrm{Ram}(B)} p$. If N is squarefree, then the p-Witt invariant is $w_p = -1$ if $p \mid D$ and $w_p = 1$ if $p \mid M = N/D$.

We have an exact sequence

$$1 \to \mathbb{Q}^\times \to B^\times \to \mathrm{SO}(V) \to 1$$

which generalizes to

$$1 \to \{\pm 1\} \to O^\times \to \mathrm{SO}(\Lambda) \to 1.$$

Sketch of proof of theorem

Sketch of proof of theorem

The even Clifford map induces a Hecke-equivariant isomorphism

Sketch of proof of theorem

The even Clifford map induces a Hecke-equivariant isomorphism

$$M(\mathrm{O}(\Lambda)) = \mathrm{Map}(\mathrm{Cl}(\Lambda), \mathbb{C}) \xrightarrow{\sim} \mathrm{Map}(\mathrm{Typ}(O), \mathbb{C})$$

where $\mathrm{Typ}(O)$ is the *type set* of O.

Sketch of proof of theorem

The even Clifford map induces a Hecke-equivariant isomorphism

$$M(\mathrm{O}(\Lambda)) = \mathrm{Map}(\mathrm{Cl}(\Lambda), \mathbb{C}) \xrightarrow{\sim} \mathrm{Map}(\mathrm{Typ}(O), \mathbb{C})$$

where $\mathrm{Typ}(O)$ is the *type set* of O.

By restricting Brandt matrices (Eichler's *Anzahlmatrizen*) we have

$$\mathrm{Map}(\mathrm{Typ}(O), \mathbb{C}) \hookrightarrow M_2(\Gamma_0(N))$$

with an image that can be explicitly identified.

Where are the other forms?

Where are the other forms?

We only get a subspace of classical modular forms this way.

Where are the other forms?

We only get a subspace of classical modular forms this way. To get them all, we add a representation.

Where are the other forms?

We only get a subspace of classical modular forms this way. To get them all, we add a representation.

More generally, let $\rho : \mathsf{O}(V) \to \mathsf{GL}(W)$ be a representation with W a finite-dimensional vector space over $\mathbb{C}$.

Where are the other forms?

We only get a subspace of classical modular forms this way. To get them all, we add a representation.

More generally, let $\rho : \mathsf{O}(V) \to \mathsf{GL}(W)$ be a representation with W a finite-dimensional vector space over $\mathbb{C}$. We refer to ρ as the **weight**.

Where are the other forms?

We only get a subspace of classical modular forms this way. To get them all, we add a representation.

More generally, let $\rho : \mathsf{O}(V) \to \mathsf{GL}(W)$ be a representation with W a finite-dimensional vector space over $\mathbb{C}$. We refer to ρ as the **weight**. For example:

Where are the other forms?

We only get a subspace of classical modular forms this way. To get them all, we add a representation.

More generally, let $\rho : \mathsf{O}(V) \to \mathsf{GL}(W)$ be a representation with W a finite-dimensional vector space over $\mathbb{C}$. We refer to ρ as the **weight**. For example:

- $\rho : \mathsf{O}(V) \to \mathbb{C}^\times$ the trivial representation.

Where are the other forms?

We only get a subspace of classical modular forms this way. To get them all, we add a representation.

More generally, let $\rho : \mathrm{O}(V) \to \mathrm{GL}(W)$ be a representation with W a finite-dimensional vector space over $\mathbb{C}$. We refer to ρ as the **weight**. For example:

- $\rho : \mathrm{O}(V) \to \mathbb{C}^\times$ the trivial representation.
- $\rho : \mathrm{O}(V) \hookrightarrow \mathrm{GL}(V)$ the standard representation.

Where are the other forms?

We only get a subspace of classical modular forms this way. To get them all, we add a representation.

More generally, let $\rho : \mathrm{O}(V) \to \mathrm{GL}(W)$ be a representation with W a finite-dimensional vector space over $\mathbb{C}$. We refer to ρ as the **weight**. For example:

- $\rho : \mathrm{O}(V) \to \mathbb{C}^\times$ the trivial representation.
- $\rho : \mathrm{O}(V) \hookrightarrow \mathrm{GL}(V)$ the standard representation.
- $\rho : \mathrm{O}(V) \to \mathrm{GL}(\mathrm{Har}_k)$ the natural change-of-variables action on degree k harmonic polynomials in 3 variables.

Spinor character

Spinor character

We have a natural homomorphism obtained from the composition

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathrm{O}(V)$$

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathsf{O}(V) \to \mathsf{O}(V)/\{\pm 1\}$$

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathsf{O}(V) \to \mathsf{O}(V)/\{\pm 1\} \to \mathsf{SO}(V)$$

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathsf{O}(V) \to \mathsf{O}(V)/\{\pm 1\} \to \mathsf{SO}(V) \simeq B^\times/\mathbb{Q}^\times$$

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathsf{O}(V) \to \mathsf{O}(V)/\{\pm 1\} \to \mathsf{SO}(V) \simeq B^\times/\mathbb{Q}^\times \xrightarrow{\mathsf{nrd}} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathsf{O}(V) \to \mathsf{O}(V)/\{\pm 1\} \to \mathsf{SO}(V) \simeq B^\times/\mathbb{Q}^\times \xrightarrow{\mathsf{nrd}} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

called the **spinor norm**.

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathrm{O}(V) \to \mathrm{O}(V)/\{\pm 1\} \to \mathrm{SO}(V) \simeq B^\times/\mathbb{Q}^\times \xrightarrow{\mathrm{nrd}} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

called the **spinor norm**.

Lemma

Let $\gamma \in \mathrm{SO}(V)$ have $\mathrm{tr}(\gamma) \neq -1$. Then the spinor norm of γ is $\mathrm{tr}(\gamma) + 1$.

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathrm{O}(V) \to \mathrm{O}(V)/\{\pm 1\} \to \mathrm{SO}(V) \simeq B^\times/\mathbb{Q}^\times \xrightarrow{\mathrm{nrd}} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

called the **spinor norm**.

Lemma

Let $\gamma \in \mathrm{SO}(V)$ have $\mathrm{tr}(\gamma) \neq -1$. Then the spinor norm of γ is $\mathrm{tr}(\gamma) + 1$.

(There are more complicated but still nice formulas in the degenerate case $\mathrm{tr}(\gamma) = -1$.)

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathrm{O}(V) \to \mathrm{O}(V)/\{\pm 1\} \to \mathrm{SO}(V) \simeq B^\times/\mathbb{Q}^\times \xrightarrow{\mathrm{nrd}} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

called the **spinor norm**.

Lemma

Let $\gamma \in \mathrm{SO}(V)$ have $\mathrm{tr}(\gamma) \neq -1$. Then the spinor norm of γ is $\mathrm{tr}(\gamma) + 1$.

(There are more complicated but still nice formulas in the degenerate case $\mathrm{tr}(\gamma) = -1$.)

For $r \mid N$, the **spinor character** for r is

$$\mathrm{spin}_r : \mathrm{O}(V) \xrightarrow{\sigma} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathrm{O}(V) \to \mathrm{O}(V)/\{\pm 1\} \to \mathrm{SO}(V) \simeq B^\times/\mathbb{Q}^\times \xrightarrow{\mathrm{nrd}} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

called the **spinor norm**.

Lemma

Let $\gamma \in \mathrm{SO}(V)$ have $\mathrm{tr}(\gamma) \neq -1$. Then the spinor norm of γ is $\mathrm{tr}(\gamma) + 1$.

(There are more complicated but still nice formulas in the degenerate case $\mathrm{tr}(\gamma) = -1$.)

For $r \mid N$, the **spinor character** for r is

$$\mathrm{spin}_r : \mathrm{O}(V) \xrightarrow{\sigma} \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \to \{\pm 1\}$$

Spinor character

We have a natural homomorphism obtained from the composition

$$\sigma : \mathrm{O}(V) \to \mathrm{O}(V)/\{\pm 1\} \to \mathrm{SO}(V) \simeq B^\times/\mathbb{Q}^\times \xrightarrow{\mathrm{nrd}} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

called the **spinor norm**.

Lemma

Let $\gamma \in \mathrm{SO}(V)$ have $\mathrm{tr}(\gamma) \neq -1$. Then the spinor norm of γ is $\mathrm{tr}(\gamma) + 1$.

(There are more complicated but still nice formulas in the degenerate case $\mathrm{tr}(\gamma) = -1$.)

For $r \mid N$, the **spinor character** for r is

$$\begin{aligned} \mathrm{spin}_r : \mathrm{O}(V) \xrightarrow{\sigma} \mathbb{Q}^\times/\mathbb{Q}^{\times 2} &\to \{\pm 1\} \\ a &\mapsto \prod_{p \mid r} (-1)^{\mathrm{ord}_p(a)} \end{aligned}$$

Orthogonal modular forms with weight

Orthogonal modular forms with weight

Let $\Lambda_1, \ldots, \Lambda_h$ represent $\mathrm{Cl}(\Lambda)$, with $\Lambda_1 = \Lambda$.

Orthogonal modular forms with weight

Let $\Lambda_1, \ldots, \Lambda_h$ represent $\mathrm{Cl}(\Lambda)$, with $\Lambda_1 = \Lambda$.

For a weight ρ, we define **orthogonal modular forms for Λ of weight ρ** to be

$$M(\mathrm{O}(\Lambda), \rho)$$

Orthogonal modular forms with weight

Let $\Lambda_1, \ldots, \Lambda_h$ represent $\mathrm{Cl}(\Lambda)$, with $\Lambda_1 = \Lambda$.

For a weight ρ, we define **orthogonal modular forms for Λ of weight ρ** to be

$$M(\mathrm{O}(\Lambda), \rho) := \{f : \mathrm{Cl}(\Lambda) \to W \mid f([\Lambda_i]) \in W^{\mathrm{O}(\Lambda_i)}\}$$

Orthogonal modular forms with weight

Let $\Lambda_1, \ldots, \Lambda_h$ represent $\mathrm{Cl}(\Lambda)$, with $\Lambda_1 = \Lambda$.

For a weight ρ, we define **orthogonal modular forms for Λ of weight** ρ to be

$$M(\mathrm{O}(\Lambda), \rho) := \{f : \mathrm{Cl}(\Lambda) \to W \mid f([\Lambda_i]) \in W^{\mathrm{O}(\Lambda_i)}\} \simeq \bigoplus_{i=1}^{h} W^{\mathrm{O}(\Lambda_i)}.$$

Orthogonal modular forms with weight

Let $\Lambda_1, \ldots, \Lambda_h$ represent $\mathrm{Cl}(\Lambda)$, with $\Lambda_1 = \Lambda$.

For a weight ρ, we define **orthogonal modular forms for Λ of weight ρ** to be

$$M(\mathrm{O}(\Lambda), \rho) := \{f : \mathrm{Cl}(\Lambda) \to W \mid f([\Lambda_i]) \in W^{\mathrm{O}(\Lambda_i)}\} \simeq \bigoplus_{i=1}^{h} W^{\mathrm{O}(\Lambda_i)}.$$

Let $p \nmid \mathrm{disc}(\Lambda)$.

Orthogonal modular forms with weight

Let $\Lambda_1, \ldots, \Lambda_h$ represent $\mathrm{Cl}(\Lambda)$, with $\Lambda_1 = \Lambda$.

For a weight ρ, we define **orthogonal modular forms for Λ of weight ρ** to be

$$M(\mathrm{O}(\Lambda), \rho) := \{f : \mathrm{Cl}(\Lambda) \to W \mid f([\Lambda_i]) \in W^{\mathrm{O}(\Lambda_i)}\} \simeq \bigoplus_{i=1}^{h} W^{\mathrm{O}(\Lambda_i)}.$$

Let $p \nmid \mathrm{disc}(\Lambda)$. For a p-neighbor $\Pi \sim_p \Lambda$, we have $\Pi = \gamma \Lambda_j$ for unique j and unique γ up to right multiplication by $\mathrm{O}(\Lambda_j)$.

Orthogonal modular forms with weight

Let $\Lambda_1, \ldots, \Lambda_h$ represent $\mathrm{Cl}(\Lambda)$, with $\Lambda_1 = \Lambda$.

For a weight ρ, we define **orthogonal modular forms for Λ of weight ρ** to be

$$M(\mathrm{O}(\Lambda), \rho) := \{f : \mathrm{Cl}(\Lambda) \to W \mid f([\Lambda_i]) \in W^{\mathrm{O}(\Lambda_i)}\} \simeq \bigoplus_{i=1}^{h} W^{\mathrm{O}(\Lambda_i)}.$$

Let $p \nmid \mathrm{disc}(\Lambda)$. For a p-neighbor $\Pi \sim_p \Lambda$, we have $\Pi = \gamma\Lambda_j$ for unique j and unique γ up to right multiplication by $\mathrm{O}(\Lambda_j)$.

Define the **Hecke operator**

$$T_p : M(\mathrm{O}(\Lambda), \rho) \to M(\mathrm{O}(\Lambda), \rho)$$

Orthogonal modular forms with weight

Let $\Lambda_1, \ldots, \Lambda_h$ represent $\mathrm{Cl}(\Lambda)$, with $\Lambda_1 = \Lambda$.

For a weight ρ, we define **orthogonal modular forms for Λ of weight ρ** to be

$$M(\mathrm{O}(\Lambda), \rho) := \{f : \mathrm{Cl}(\Lambda) \to W \mid f([\Lambda_i]) \in W^{\mathrm{O}(\Lambda_i)}\} \simeq \bigoplus_{i=1}^{h} W^{\mathrm{O}(\Lambda_i)}.$$

Let $p \nmid \mathrm{disc}(\Lambda)$. For a p-neighbor $\Pi \sim_p \Lambda$, we have $\Pi = \gamma\Lambda_j$ for unique j and unique γ up to right multiplication by $\mathrm{O}(\Lambda_j)$.

Define the **Hecke operator**

$$\begin{aligned} T_p : M(\mathrm{O}(\Lambda), \rho) &\to M(\mathrm{O}(\Lambda), \rho) \\ T_p(f)([\Lambda']) & \end{aligned}$$

Orthogonal modular forms with weight

Let $\Lambda_1, \ldots, \Lambda_h$ represent $\mathrm{Cl}(\Lambda)$, with $\Lambda_1 = \Lambda$.

For a weight ρ, we define **orthogonal modular forms for Λ of weight ρ** to be

$$M(\mathrm{O}(\Lambda), \rho) := \{f : \mathrm{Cl}(\Lambda) \to W \mid f([\Lambda_i]) \in W^{\mathrm{O}(\Lambda_i)}\} \simeq \bigoplus_{i=1}^{h} W^{\mathrm{O}(\Lambda_i)}.$$

Let $p \nmid \mathrm{disc}(\Lambda)$. For a p-neighbor $\Pi \sim_p \Lambda$, we have $\Pi = \gamma\Lambda_j$ for unique j and unique γ up to right multiplication by $\mathrm{O}(\Lambda_j)$.

Define the **Hecke operator**

$$\begin{aligned} T_p : M(\mathrm{O}(\Lambda), \rho) &\to M(\mathrm{O}(\Lambda), \rho) \\ T_p(f)([\Lambda']) &:= \sum_{\gamma'\Lambda_j = \Pi' \sim_p \Lambda'} f([\Pi'])^{\gamma'}. \end{aligned}$$

Orthogonal modular forms with weight

Let $\Lambda_1, \ldots, \Lambda_h$ represent $\mathrm{Cl}(\Lambda)$, with $\Lambda_1 = \Lambda$.

For a weight ρ, we define **orthogonal modular forms for Λ of weight ρ** to be

$$M(\mathrm{O}(\Lambda), \rho) := \{f : \mathrm{Cl}(\Lambda) \to W \mid f([\Lambda_i]) \in W^{\mathrm{O}(\Lambda_i)}\} \simeq \bigoplus_{i=1}^{h} W^{\mathrm{O}(\Lambda_i)}.$$

Let $p \nmid \mathrm{disc}(\Lambda)$. For a p-neighbor $\Pi \sim_p \Lambda$, we have $\Pi = \gamma \Lambda_j$ for unique j and unique γ up to right multiplication by $\mathrm{O}(\Lambda_j)$.

Define the **Hecke operator**

$$\begin{aligned} T_p : M(\mathrm{O}(\Lambda), \rho) &\to M(\mathrm{O}(\Lambda), \rho) \\ T_p(f)([\Lambda']) &:= \sum_{\gamma' \Lambda_j = \Pi' \sim_p \Lambda'} f([\Pi'])^{\gamma'}. \end{aligned}$$

The Hecke operators generate a commutative, semisimple ring.

Modular forms: first theorem

Modular forms: first theorem

Theorem (Hein–Tornaría–V)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree.

Modular forms: first theorem

Theorem (Hein–Tornaría–V)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree. Let $\epsilon_p \in \{\pm 1\}$ be the p-Witt invariant for $p \mid N$ and let $D = \prod_{p : \epsilon_p = -1} p$.

Modular forms: first theorem

Theorem (Hein–Tornaría–V)

Suppose $N = \operatorname{disc}(\Lambda)$ is squarefree. Let $\epsilon_p \in \{\pm 1\}$ be the p-Witt invariant for $p \mid N$ and let $D = \prod_{p : \epsilon_p = -1} p$.

Let $r \mid N$, and for $p \mid N$ let $\epsilon'_p = 1, -1$ as $p \nmid r$ or $p \mid r$.

Modular forms: first theorem

Theorem (Hein–Tornaría–V)

Suppose $N = \mathrm{disc}(\Lambda)$ is squarefree. Let $\epsilon_p \in \{\pm 1\}$ be the p-Witt invariant for $p \mid N$ and let $D = \prod_{p : \epsilon_p = -1} p$.

Let $r \mid N$, and for $p \mid N$ let $\epsilon'_p = 1, -1$ as $p \nmid r$ or $p \mid r$.

Then there is a Hecke-equivariant isomorphism

$$S(\mathrm{O}(\Lambda), \rho) \xrightarrow{\sim} S_2(\Gamma_0(N); D\text{-new}; w = \epsilon').$$

Computational results

Computational results

For level $N = 1062347 = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ and $D = N$ (so all forms are new),

Computational results

For level $N = 1062347 = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ and $D = N$ (so all forms are new), we take

$$Q(x, y, z) = x^2 + 187y^2 + 1467z^2 - 187xz$$

and have $\# \operatorname{Cl}(\Lambda) = 2016$.

Computational results

For level $N = 1062347 = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ and $D = N$ (so all forms are new), we take

$$Q(x, y, z) = x^2 + 187y^2 + 1467z^2 - 187xz$$

and have $\# \operatorname{Cl}(\Lambda) = 2016$.

Given Q, we can compute $[T_2], [T_3], [T_5], [T_7]$ for *all* characters (giving all newforms) in 4 seconds on a standard desktop machine.

Computational results

For level $N = 1062347 = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ and $D = N$ (so all forms are new), we take

$$Q(x, y, z) = x^2 + 187y^2 + 1467z^2 - 187xz$$

and have $\# \mathrm{Cl}(\Lambda) = 2016$.

Given Q, we can compute $[T_2], [T_3], [T_5], [T_7]$ for *all* characters (giving all newforms) in 4 seconds on a standard desktop machine. Then 1 minute of linear algebra computing kernels with sparse matrices in Magma gives that there are exactly 5 elliptic curves with conductor N.

Computational results

For level $N = 1062347 = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ and $D = N$ (so all forms are new), we take

$$Q(x, y, z) = x^2 + 187y^2 + 1467z^2 - 187xz$$

and have $\# \mathrm{Cl}(\Lambda) = 2016$.

Given Q, we can compute $[T_2], [T_3], [T_5], [T_7]$ for *all* characters (giving all newforms) in 4 seconds on a standard desktop machine. Then 1 minute of linear algebra computing kernels with sparse matrices in Magma gives that there are exactly 5 elliptic curves with conductor N.

This isn't a "generic" level!

Computational results

For level $N = 1062347 = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ and $D = N$ (so all forms are new), we take

$$Q(x, y, z) = x^2 + 187y^2 + 1467z^2 - 187xz$$

and have $\# \mathrm{Cl}(\Lambda) = 2016$.

Given Q, we can compute $[T_2], [T_3], [T_5], [T_7]$ for *all* characters (giving all newforms) in 4 seconds on a standard desktop machine. Then 1 minute of linear algebra computing kernels with sparse matrices in Magma gives that there are exactly 5 elliptic curves with conductor N.

This isn't a "generic" level! But to make an unfair comparison: the same computation with modular symbols in Magma crashed after consuming all 24 GB of available memory.

Relationship to Mestre–Oesterlé

Relationship to Mestre–Oesterlé

To tie up the motivating thread...

Relationship to Mestre–Oesterlé

To tie up the motivating thread...

Lemma

Let O be a maximal order in a quaternion algebra B with discriminant $\mathrm{disc}(B) = p$.

Relationship to Mestre–Oesterlé

To tie up the motivating thread...

Lemma

Let O be a maximal order in a quaternion algebra B with discriminant $\mathrm{disc}(B) = p$. Then there exist one or two supersingular curves E up to isomorphism over $\overline{\mathbb{F}}_p$ such that $\mathrm{End}(E) \simeq O$.

Relationship to Mestre–Oesterlé

To tie up the motivating thread...

Lemma

Let O be a maximal order in a quaternion algebra B with discriminant $\mathrm{disc}(B) = p$. Then there exist one or two supersingular curves E up to isomorphism over $\overline{\mathbb{F}}_p$ such that $\mathrm{End}(E) \simeq O$.

There exist two such elliptic curves if and only if $j(E) \in \mathbb{F}_{p^2} \smallsetminus \mathbb{F}_p$ if and only if the unique two-sided ideal of O of reduced norm p is not principal.

Relationship to Mestre–Oesterlé

To tie up the motivating thread...

Lemma

Let O be a maximal order in a quaternion algebra B with discriminant $\mathrm{disc}(B) = p$. Then there exist one or two supersingular curves E up to isomorphism over $\overline{\mathbb{F}}_p$ such that $\mathrm{End}(E) \simeq O$.

There exist two such elliptic curves if and only if $j(E) \in \mathbb{F}_{p^2} \smallsetminus \mathbb{F}_p$ if and only if the unique two-sided ideal of O of reduced norm p is not principal.

So the spinor characters account exactly for the identification of E with its Galois conjugate $\phi(E)$ when $j(E) \notin \mathbb{F}_p$;

Relationship to Mestre–Oesterlé

To tie up the motivating thread...

Lemma

Let O be a maximal order in a quaternion algebra B with discriminant $\operatorname{disc}(B) = p$. Then there exist one or two supersingular curves E up to isomorphism over $\overline{\mathbb{F}}_p$ such that $\operatorname{End}(E) \simeq O$.

There exist two such elliptic curves if and only if $j(E) \in \mathbb{F}_{p^2} \smallsetminus \mathbb{F}_p$ if and only if the unique two-sided ideal of O of reduced norm p is not principal.

So the spinor characters account exactly for the identification of E with its Galois conjugate $\phi(E)$ when $j(E) \notin \mathbb{F}_p$; the two are distinguished by an *orientation*, following Ribet.

Extensions

Extensions

To work with level N, we design a suitable lattice locally subject to a global compatibility (Hilbert reciprocity).

Extensions

To work with level N, we design a suitable lattice locally subject to a global compatibility (Hilbert reciprocity).

A definite quadratic form Q which is locally isometric to $xy + Nz^2$ for all primes p would work,

Extensions

To work with level N, we design a suitable lattice locally subject to a global compatibility (Hilbert reciprocity).

A definite quadratic form Q which is locally isometric to $xy + Nz^2$ for all primes p would work, but this does not satisfy global compatibility.

Extensions

To work with level N, we design a suitable lattice locally subject to a global compatibility (Hilbert reciprocity).

A definite quadratic form Q which is locally isometric to $xy + Nz^2$ for all primes p would work, but this does not satisfy global compatibility.

We need a prime power $p^e \parallel N$ with e odd to ensure global compatibility,

Extensions

To work with level N, we design a suitable lattice locally subject to a global compatibility (Hilbert reciprocity).

A definite quadratic form Q which is locally isometric to $xy + Nz^2$ for all primes p would work, but this does not satisfy global compatibility.

We need a prime power $p^e \parallel N$ with e odd to ensure global compatibility, and use instead a form isometric over $\mathbb{Q}_p$ to $x^2 - uy^2 + Nz^2$ where u is a nonsquare modulo $p \neq 2$ (and $x^2 + xy + y^2 + Nz^2$ for $p = 2$).

Extensions

To work with level N, we design a suitable lattice locally subject to a global compatibility (Hilbert reciprocity).

A definite quadratic form Q which is locally isometric to $xy + Nz^2$ for all primes p would work, but this does not satisfy global compatibility.

We need a prime power $p^e \parallel N$ with e odd to ensure global compatibility, and use instead a form isometric over $\mathbb{Q}_p$ to $x^2 - uy^2 + Nz^2$ where u is a nonsquare modulo $p \neq 2$ (and $x^2 + xy + y^2 + Nz^2$ for $p = 2$). The corresponding quaternion order $\mathcal{O}$ was investigated by Pizer; it is called *residually inert*, as $\mathcal{O}/\text{rad}(\mathcal{O}) \simeq \mathbb{F}_{p^2}$, where $\text{rad}(\mathcal{O})$ is the Jacobson radical.

Extensions

To work with level N, we design a suitable lattice locally subject to a global compatibility (Hilbert reciprocity).

A definite quadratic form Q which is locally isometric to $xy + Nz^2$ for all primes p would work, but this does not satisfy global compatibility.

We need a prime power $p^e \parallel N$ with e odd to ensure global compatibility, and use instead a form isometric over $\mathbb{Q}_p$ to $x^2 - uy^2 + Nz^2$ where u is a nonsquare modulo $p \neq 2$ (and $x^2 + xy + y^2 + Nz^2$ for $p = 2$). The corresponding quaternion order O was investigated by Pizer; it is called *residually inert*, as $O/\mathrm{rad}(O) \simeq \mathbb{F}_{p^2}$, where $\mathrm{rad}(O)$ is the Jacobson radical.

We can also work over a totally real field F to obtain Hilbert modular forms, with the same techniques and analogous statements of running time.

Modular forms: main theorem

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

a weight $k \in 2\mathbb{Z}_{>0}$,

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

a weight $k \in 2\mathbb{Z}_{>0}$,
a factored *nonsquare* level $N = \prod_i p_i^{e_i}$,

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

$$\text{a weight } k \in 2\mathbb{Z}_{>0},$$
$$\text{a factored } \textit{nonsquare} \text{ level } N = \textstyle\prod_i p_i^{e_i},$$
$$D \mid \textstyle\prod_{2\nmid e_i} p_i \quad \text{with an } \textit{odd} \text{ number of factors,}$$

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

$$\text{a weight } k \in 2\mathbb{Z}_{>0},$$
$$\text{a factored } \textit{nonsquare} \text{ level } N = \prod_i p_i^{e_i},$$
$$D \mid \prod_{2\nmid e_i} p_i \quad \text{with an } \textit{odd} \text{ number of factors,}$$
$$\text{and } \epsilon \in \{\pm 1\}^r,$$

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

$$\begin{gathered}\text{a weight } k \in 2\mathbb{Z}_{>0},\\ \text{a factored } \textit{nonsquare} \text{ level } N = \textstyle\prod_i p_i^{e_i},\\ D \mid \textstyle\prod_{2\nmid e_i} p_i \;\; \text{with an } \textit{odd} \text{ number of factors,}\\ \text{and } \epsilon \in \{\pm 1\}^r,\end{gathered}$$

computes as output the space $S_k(\Gamma_0(N); D\text{-new}; w = \epsilon)$ as a Hecke module.

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

$$\begin{gathered}\text{a weight } k \in 2\mathbb{Z}_{>0},\\ \text{a factored } \textit{nonsquare} \text{ level } N = \textstyle\prod_i p_i^{e_i},\\ D \mid \textstyle\prod_{2\nmid e_i} p_i \;\; \text{with an } \textit{odd} \text{ number of factors},\\ \text{and } \epsilon \in \{\pm 1\}^r,\end{gathered}$$

computes as output the space $S_k(\Gamma_0(N); D\text{-new}; w = \epsilon)$ as a Hecke module.

After precomputation steps (hard to analyze, instantaneous in practice),

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

$$\begin{gathered}\text{a weight } k \in 2\mathbb{Z}_{>0}, \\ \text{a factored \textit{nonsquare} level } N = \prod_i p_i^{e_i}, \\ D \mid \prod_{2 \nmid e_i} p_i \ \text{ with an \textit{odd} number of factors,} \\ \text{and } \epsilon \in \{\pm 1\}^r,\end{gathered}$$

computes as output the space $S_k(\Gamma_0(N); D\text{-new}; w = \epsilon)$ as a Hecke module.

After precomputation steps (hard to analyze, instantaneous in practice), the running time of the algorithm to compute T_p is $\widetilde{O}(pd)$,

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

$$\begin{gathered} \text{a weight } k \in 2\mathbb{Z}_{>0}, \\ \text{a factored } \textit{nonsquare} \text{ level } N = \prod_i p_i^{e_i}, \\ D \mid \prod_{2\nmid e_i} p_i \;\; \text{with an } \textit{odd} \text{ number of factors,} \\ \text{and } \epsilon \in \{\pm 1\}^r, \end{gathered}$$

computes as output the space $S_k(\Gamma_0(N); D\text{-new}; w = \epsilon)$ as a Hecke module.

After precomputation steps (hard to analyze, instantaneous in practice), the running time of the algorithm to compute T_p is $\widetilde{O}(pd)$, where

$d = \dim S(\mathrm{O}(\Lambda), \rho)$

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

a weight $k \in 2\mathbb{Z}_{>0}$,
a factored *nonsquare* level $N = \prod_i p_i^{e_i}$,
$D \mid \prod_{2 \nmid e_i} p_i$ with an *odd* number of factors,
and $\epsilon \in \{\pm 1\}^r$,

computes as output the space $S_k(\Gamma_0(N); D\text{-new}; w = \epsilon)$ as a Hecke module.

After precomputation steps (hard to analyze, instantaneous in practice), the running time of the algorithm to compute T_p is $\widetilde{O}(pd)$, where

$$d = \dim S(\mathrm{O}(\Lambda), \rho) = \dim S_k(\Gamma_0(N); D\text{-new}; w = \epsilon)$$

Modular forms: main theorem

Theorem (Hein–Tornaría–V)

There exists an explicit, deterministic algorithm that, given as input

$$\begin{gathered} \text{a weight } k \in 2\mathbb{Z}_{>0}, \\ \text{a factored } \textit{nonsquare} \text{ level } N = \textstyle\prod_i p_i^{e_i}, \\ D \mid \textstyle\prod_{2\nmid e_i} p_i \ \text{ with an } \textit{odd} \text{ number of factors,} \\ \text{and } \epsilon \in \{\pm 1\}^r, \end{gathered}$$

computes as output the space $S_k(\Gamma_0(N); D\text{-new}; w = \epsilon)$ as a Hecke module.

After precomputation steps (hard to analyze, instantaneous in practice), the running time of the algorithm to compute T_p is $\widetilde{O}(pd)$, where

$$d = \dim S(\mathrm{O}(\Lambda), \rho) = \dim S_k(\Gamma_0(N); D\text{-new}; w = \epsilon) = O(2^{-r} kN).$$

Conclusion

Conclusion

- Birch's method for computing modular forms can be understood intrinsically in the language of orthogonal modular forms.

Conclusion

- Birch's method for computing modular forms can be understood intrinsically in the language of orthogonal modular forms.
- This method then generalizes to capture classical (and Hilbert) modular forms with nonsquare level in a natural way by adding a representation.

Conclusion

- Birch's method for computing modular forms can be understood intrinsically in the language of orthogonal modular forms.
- This method then generalizes to capture classical (and Hilbert) modular forms with nonsquare level in a natural way by adding a representation.
- The implementation is *very fast*!

Conclusion

- Birch's method for computing modular forms can be understood intrinsically in the language of orthogonal modular forms.
- This method then generalizes to capture classical (and Hilbert) modular forms with nonsquare level in a natural way by adding a representation.
- The implementation is *very fast*!

Thank you to the CIRM for 30+ years of algorithmic arithmetic geometry!