LATTICE METHODS IN MODULARITY

ERAN ASSAF

1. Representation Numbers

Let $Q(x) = \sum_{i \le j}^{k} a_{ij} x_i x_j \in \mathbb{Z}[x_1, \ldots, x_k]$ be a positive definite quadratic form. Write $r_Q(n) = \#\{\lambda \in \mathbb{Z}^k : Q(\lambda) = n\}$.

Question 1.1. *Is there a "nice" formula for $r_Q(n)$?*

Example 1.2 (Jacobi, 1834)**.** Let $Q(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Then

$$r_Q(n) = 8 \sum_{4 \nmid d | n} d.$$

Jacobi's original proof, as well as many subsequent proofs, relies heavily on certain identities he had developed that somewhat obfuscate the underlying ideas. I'll present here two different proofs, that will be easier to generalize and have analogues in different situations.

Proof Sketch. The main line of all these proofs looks as follows.

- Consider $\theta(q) = \sum_{n=0}^{\infty} r_Q(n) q^n$.
- Exhibit a f.d. vector space V s.t. $\theta \in V$.
- Find a "nice" basis for V.
- Write θ as a linear combination of basis elements.

Possible choices for V - spaces of elliptic functions or spaces of modular forms. $\square$

Alternatively, one could prove this directly using arithmetic in quaternion algebras.

Proof #2 Sketch. Let B be the (Hamilton) quaternion algebra over $\mathbb{Q}$, namely $B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ is a 4-dim. algebra over $\mathbb{Q}$ with basis $\{1, i, j, ij\}$ such that $i^2 = -1 = j^2$ and $ji = -ij$. Let $O = \mathbb{Z}\langle i, j \rangle$ be the (Lipshitz) order generated by i, j. Then

$$r_Q(n) = \#\{\beta \in O : \operatorname{nrd}(\beta) = n\}.$$

- It turns out that all invertible (sated) O-ideals are principal.
- $\#O^\times = 8$.

So $r_Q(n) = 8 \cdot \#\{I \in \operatorname{Cls}(O) : \operatorname{nrd}(I) = n\}$. This last quantity is multiplicative, so it is enough to compute it for prime powers.

- For $p \neq 2$, we have $O_p \simeq M_2(\mathbb{Z}_p)$, so right ideals of norm p^r correspond to submodules of $(\mathbb{Z}/p^r\mathbb{Z})^2$ of index p^r.

- For $p = 2$, a direct count shows there are exactly 3 such inequivalent ideals.

Multiplying all together yields the result. □

Question 1.3. *What about other quadratic forms?*

for that we will change our point of view slightly, and talk about lattices.

2. Lattices

Let V be a finite dimensional vector space over $\mathbb{Q}$, and let $Q : V \to \mathbb{Q}$ be a quadratic form. Let $\Lambda \subseteq V$ be an even integral lattice (so that $Q(\Lambda) \subseteq \mathbb{Z}$). Write $T(x, y) = Q(x + y) - Q(x) - Q(y)$ for the associated bilinear form (polar). The discriminant of Λ is $D = \mathrm{disc}(\Lambda) = 2^{-\epsilon} \det T \in Z$, where $\epsilon = k \bmod 2$. The level of Λ is the smallest N s.t. NT^{-1} is integral with even diagonal. Set

$$\theta_\Lambda(q) = \sum_{\lambda \in \Lambda} q^{Q(\lambda)} = \sum_{n=0}^{\infty} r_\Lambda(n) q^n,$$

where $r_\Lambda(n) = \#\{\lambda \in \Lambda : Q(\lambda) = n\}$, and let $D^* = D$ if $2 \nmid k$ or $D^* = (-1)^{k/2} D$ if $2 \mid k$, and $\chi_D(a) = \left(\frac{D}{a}\right)$. Then it is a theorem (Freitag, 1983) that

$$\theta_\Lambda(q) \in M_{k/2}(N, \chi_{D^*}).$$

Example 2.1. Let $V = \mathbb{Q}^3$, with $Q(x, y, z) = x^2 + y^2 + yz + 3z^2$ and let $\Lambda = \mathbb{Z}^3$. Then

$$[T]_B = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 6 \end{pmatrix}, \quad B = \{e_1, e_2, e_3\}.$$

and similarly

$$[T]_{B'} = \begin{pmatrix} 8 & 1 & 6 \\ 1 & 2 & 1 \\ 6 & 1 & 6 \end{pmatrix}, \quad B' = \{e_1 + e_3, e_2, e_3\}.$$

Note that $\det(T) = 22$, so that $\mathrm{disc}(\Lambda) = 11$. From $[T]_B^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{11}\begin{pmatrix} 6 & -1 \\ -1 & 2 \end{pmatrix} \end{pmatrix}$, we get that $N = 44$. Therefore

$$\theta_\Lambda(q) = 1 + 4q + 4q^2 + 4q^3 + 12q^4 + 12q^5 + O(q^6) \in M_{3/2}(44, \chi_{11}).$$

This observation, other than leading us to "nice" formulas for representation numbers and relations between such, leads us to try and consider these generating functions instead of the lattices. This is a good time to ask the following question.

Question 2.2. *Is $\Lambda \mapsto \theta_\Lambda$ injective?*

The answer to this question is clearly "No", because if $g \in O(V, Q)$ is an isometry ($Q(gv) = Q(v)$), then clearly $\theta_{g(\Lambda)} = \theta_\Lambda$. Let us then refine the question.

Question 2.3. *Is $[\Lambda] \mapsto \theta_\Lambda$ injective when $[\Lambda]$ is the isometry class of Λ?*

In fact, if $\Lambda \simeq \Pi$ are isometric, they are also locally isometric at every prime p (namely $\Lambda_p \simeq \Pi_p$), so we can restrict our attention to smaller sets of lattices. We can write down

$$\mathrm{Gen}(\Lambda) = \{\Pi \subseteq V : \Pi_p \simeq \Lambda_p \forall p\}$$

for the genus of Λ, and $\mathrm{Cls}(\Lambda) = \mathrm{Gen}(\Lambda)/O(V)$ for its class set. Classical geometry of numbers shows that $\mathrm{Cls}(\Lambda)$ is finite, and we obtain a well defined map $\theta : \mathrm{Cls}(\Lambda) \to M_{k/2}(N, \chi_{D^*})$, which we would like to figure out if it is injective.

Remark 2.4. For those who are more adelically inclined, one could think of the class set as an adelic double coset for the algebraic group $O(V)$ as $O(V)\backslash O(\widehat{V})/O(\widehat{\Lambda})$.

Example 2.5. The map $\theta : \mathrm{Cls}(\Lambda) \to M_{k/2}(N, \chi_{D^*})$ is not injective. Indeed, consider the lattice $D_k = \{x \in \mathbb{Z}^k : 2 \mid \sum_{i=1}^k x_i\}$, and write $E_k = D_k + \mathbb{Z} \cdot v$ where $v = \frac{1}{2}(1, \ldots, 1) \in \mathbb{Q}^k$. Then $\mathrm{disc}(E_8) = \mathrm{disc}(E_{16}) = 1$, and $\theta_{E_{16}}, \theta_{E_8 \boxplus E_8} \in M_8(1)$. But $\dim M_8(1) = 1$, hence the theta series are equal, but in fact these two lattices are not isometric. How does one show that? One way is to compute sizes of automorphism groups and notice they differ.

Another way to see that these lattices are not isometric is by considering the following refinement. Instead of creating a generating series by looping over single vectors in Λ, we will create a multivariate generating series by looping over sets of g vectors in Λ, namely

$$\theta_\Lambda^{(g)}(z) = \sum_{\lambda_1, \ldots, \lambda_g} e^{\pi i \, \mathrm{tr}(\lambda^t T \lambda z)},$$

where $z \in \mathcal{H}_g = \{z \in M_g(\mathbb{C}) : z^t = z, \Im(z) > 0\}$ is in the Siegel upper half-space. Again, one has a theorem

$$\theta_\Lambda^{(g)} \in M_{k/2}^{(g)}(N, \chi_{D^*}),$$

where this time this is a corresponding space of holomorphic Siegel modular forms (of degree g) of level N, weight $k/2$ and character χ_{D^*}. (Sections of an automorphic line bundle on the moduli space of abelian varieties of dimension g). Still one obtains $\theta_{E_{16}}^{(g)} = \theta_{E_8 \boxplus E_8}^{(g)}$ for $g = 1, 2, 3$, since $\dim S_8^{(g)}(1) = 0$ for $g = 1, 2, 3$. But for $g = 4$ one obtains an inequality.

3. Modular forms

All these previous ideas of working with lattices made use of a map to a finite dimensional space of (Siegel) modular forms, which is not always well-behaved. But, in fact, we can form a space of modular forms without losing any information. The space of orthogonal modular forms of level Λ is

$$M(\Lambda) = \{\phi : \mathrm{Cls}(\Lambda) \to \mathbb{C}\} \simeq \mathbb{C}^{h(\Lambda)}.$$

How did we gain anything from forming this vector space? The idea is that it has an additional structure. (This was already observed by Kneser in 1956).

A lattice $\Pi \subseteq V$ is a p-neighbor of Λ, denoted by $\Pi \sim_p \Lambda$ if Π is integral and $[\Lambda : \Lambda \cap \Pi] = p = [\Pi : \Lambda \cap \Pi]$. (Draw!).

Lemma 3.1. $\Pi \sim_p \Lambda \Rightarrow \Pi \in \mathrm{Gen}(\Lambda)$.

From the theory of invariant factors we deduce that there is a basis $e_1, \dots, e_n$ of Λ such that $\frac{1}{p}e_1, pe_2, e_3, \dots, e_n$ is a basis of Π. Since Π is integral it follows that $p^2 \mid Q(e_1)$, so that p-neighbors are in bijective correspondence with isotropic lines in $\Lambda/p\Lambda$ via $\Pi \mapsto \mathbb{F}_p \cdot \overline{e}_1$.

Example 3.2. If $k = 3$, $Q_{\mathbb{F}_p} \simeq \mathbb{P}^1_{\mathbb{F}_p} \Rightarrow \#Q(\mathbb{F}_p) = p + 1$ (for $p \nmid \Delta$), E.g. if $Q(x, y, z) = x^2 + y^2 + yz + 3z^2 \equiv 0 \bmod 2$, then

$$(x : y : z) \in \{(1 : 0 : 1), (1 : 1 : 0), (1 : 1 : 1)\}$$

lift to

$$v \in \{(1, 0, 1), (1, 1, 2), (1, -1, 1)\} \quad (Q(v) \equiv 0 \bmod 4).$$

Constructing the 2-neighbor corresponding to $(1, 0, 1) = e_1 + e_3$, we recall that

$$[T]_{B'} = \begin{pmatrix} 8 & 1 & 6 \\ 1 & 2 & 1 \\ 6 & 1 & 6 \end{pmatrix}$$

Dividing the first vector by 2, and multiplying the second one we obtain

$$\begin{pmatrix} 2 & 1 & 3 \\ 1 & 8 & 2 \\ 3 & 2 & 6 \end{pmatrix} \simeq \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 8 \end{pmatrix}$$

[Draw the neighbors graph - $(1 : 1 : 0)$ keeps Λ_1 in place, $(1 : 0 : 1)$ and $(1 : 1 : 1)$ send it to Λ_2, all arrows from Λ_2 get sent to Λ_1.] That way we get the adjacency matrix $[T_2] = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$ Similarly, one can compute 3-neighbors and 5-neighbors to obtain $[T_3] = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$ and $[T_5] = \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}$

These adjacency matrices can be extended to linear operators on the vector space spanned by the isometry classes.

$$T_p(f)([\Pi]) = \sum_{\Lambda' \sim_p \Pi} f([\Lambda']).$$

These commute and they are self-adjoint, hence give rise to simultaneous eigenvectors, which we call eigenforms.

Example 3.3. Returning to the quadratic form $Q = x^2 + y^2 + yz + 3z^2$, we see that we have two eigenvectors $e = (1, 1)$ and $f = (2, -3)$. For $p \neq 11$, we get that $T_p(e) = (p + 1)e$ and $T_p(f) = a_p f$, where

$$a_2 = -2, a_3 = -1, a_5 = 1, \dots$$

In fact,

$$f(q) = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = \sum_{n=1}^{\infty} a_n q^n \in S_2(11)^*.$$

or, if $E : y^2 + y = x^3 - x^2$, then $a_p = p + 1 - \#E(\mathbb{F}_p)$ for all $p \neq 11$.

Example 3.4. In $M(E_{16})$, one has $\phi = (286, -405)$ satisfying $T_p\phi = (p^4 \cdot \frac{p^7-1}{p-1} + p^7 + \tau(p) \cdot \frac{p^4-1}{p-1})$, where

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

* This is an example of an exceptional isomorphism $\mathfrak{so}_3 \simeq \mathfrak{sl}_2$ ($B_1 = A_1$). It generalizes to the following result.

Theorem 3.5 (Birch, Hein, Hein-Tornaria-Voight)**.** *If* $\operatorname{rank}(\Lambda) = 3$*,* D *is square-free, then* $S_{k-2}(\Lambda) \hookrightarrow S_k(D)$ *is Hecke-equivariant (+explicitly describe the image).*

Since $\mathfrak{so}_4 \simeq \mathfrak{sl}_2 \times \mathfrak{sl}_2$ ($D_2 = A_1 \times A_1$), also get

Theorem 3.6 (A. , Fretwell, Ingalls, Logan, Secord, Voight, 2022)**.** *If* $\operatorname{rank}(\Lambda) = 4$ *and* $\operatorname{rank}(\Lambda/p\Lambda) \geq 2$ *for all* p*, let* $F = \mathbb{Q}[\sqrt{D}]$*, and* $D = D_0 N^2$*, then*

$$S_{\frac{k_1+k_2}{2}, \frac{k_1-k_2}{2}}(\Lambda) \hookrightarrow S_{k_1,k_2}(N\mathbb{Z}_F)_{\mathrm{Gal}_F}$$

is Hecke-equivariant (and explicitly describes the image).

4. L-functions

The spaces $M_k(N, \chi)$ also admit Hecke operators T_p and $S_k(N, \chi)$ has a basis of eigenforms

$$f = \sum_{n=1}^{\infty} a_n q^n \quad a_1 = 1,$$

which give rise to L-functions

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p L_p(f,s) = \prod_p (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1}$$

This L-function converges in a right half-plane, and completing to a function $\Lambda(f,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s) = (-1)^{k/2} \cdot \varepsilon(f)\Lambda(f, k-s)$ where $\varepsilon(f) \in \{\pm 1\}$ is a sign that only depends on f.

The functional equation then allows one to analytically continue the L-function to an entire function on the complex plane, and consider its values along the critical line (line of symmetry), and the special point.

By a theorem of Eichler and Shimura (1973), when $k = 2$, $L(f,s) = L(E,s)$ for some elliptic curve $E/\mathbb{Q}$. The modularity theorem (2001) states the converse - given an elliptic curve over $\mathbb{Q}$, there exists a weight 2 modular form giving the same L-function. This allows one to deduce that the L-functions of these admit holomorphic continuation and their value at the special point is conjectured to relate to many arithmetic invariants via the BSD conjecture.

Modularity is explained by a deeper connection between E and f that can be expressed in terms of representation theory. The fact that E is defined over $\mathbb{Q}$ gives us an associated

Galois representation $\rho_E : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$, which in turn gives rise to an associated L-series $L(\rho_E, s) = L(E, s)$. Similarly, f gives rise to an automorphic representation π_f of PGL_2, for which $L(\pi_f, s) = L(f, s)$. Modularity then follows from an association between ρ_E and π_f where the Frobenius Fr_p on E corresponds to the Hecke operator T_p on f.

For Siegel modular forms $f \in S_{k,j}^{(2)}(N, \chi)$ one can also associate an L-series $L(f, s)$.

Conjecture 4.1. *(Modularity of Calabi-Yau threefolds) If X is a (rigid) Calabi-Yau threefold of conductor N, then there is a Siegel paramodular form f of weight $(3, 0)$ and level N such that $L(f, s) = L(X, s)$.*

In recent work, with Ladd, Rama, Tornaría and Voight, used the exceptional isomorphism for $\mathrm{rank}(\Lambda) = 5$

$$\mathfrak{so}_5 \simeq \mathfrak{sp}_4 \quad (B_2 = C_2)$$

to build a database of Siegel modular forms of weight 3, matching them up with corresponding varieties X. In a work in progress we prove modularity of these threefolds.

5. Langlands parametrization

Langlands' reciprocity conjecture relates automorphic representations (of a group G) and Galois representations (maps from $\mathrm{Gal}_{\mathbb{Q}}$ to the Langlands dual $\widehat{G}$). The relation uses a parametrization of the automorphic representations using conjugacy classes of semisimple elements in $\widehat{G}$ which should correspond to the image of Frobenius.

For example, if $f \in S_k(N, \chi)$ is a modular form of weight k, write $a_p(f) = p^{\frac{k-1}{2}}(\alpha_p + \alpha_p^{-1}) \quad (= a_p(\pi_f))$. Then the Satake parameter at p is

$$c_p(\pi_f) = \begin{pmatrix} \alpha_p & \\ & \alpha_p^{-1} \end{pmatrix}.$$

Similarly, one can define a Satake parameter at infinity viza

$$c_\infty(\pi_f) = z \mapsto \begin{pmatrix} \left(\frac{z}{|z|}\right)^{\frac{k-1}{2}} & \\ & \left(\frac{|z|}{z}\right)^{\frac{k-1}{2}} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$$

It turns out (an instance of functoriality in the Langlands program) that for any $d \geq 1$ there exists an automorphic representation $\pi_f[d]$ of PGL_{2d} with parameters

$$c_\infty(\pi_f[d]) = c_\infty(\pi) \otimes \mathrm{Sym}^{d-1} \begin{pmatrix} \left(\frac{z}{|z|}\right)^{\frac{1}{2}} & \\ & \left(\frac{|z|}{z}\right)^{\frac{1}{2}} \end{pmatrix} \in \mathrm{SL}_{2d}(\mathbb{C})$$

at infinity and

$$c_p(\pi_f[d]) = c_p(\pi) \otimes \mathrm{Sym}^{d-1} \begin{pmatrix} p^{\frac{1}{2}} & \\ & p^{-\frac{1}{2}} \end{pmatrix} \in \mathrm{SL}_{2d}(\mathbb{C}).$$

at the finite places. Here, for $G = \mathrm{PGL}_{2d}$, the Satake parameters lie in $\widehat{G} = \mathrm{SL}_{2d}(\mathbb{C})$.

More generally, we have the following conjecture.

Conjecture 5.1 (Langlands, Arthur, 1989, 2013). *Let G be semisimple, $r : \widehat{G} \to \mathrm{SL}_n(\mathbb{C})$ a representation. If $\pi \in \Pi_{\mathrm{disc}}(G)$, then*

$$r(c(\pi)) = c(\pi_1[d_1] \oplus \pi_2[d_2] \oplus \ldots \oplus \pi_m[d_m]).$$

This includes a further specification of the possible d_i and conditions on the π_i, that explicitly describe the image.

Some cases have been proven by Arthur and Taïbi (2015). For the case we are considering today, of a compact orthogonal group, Chenevier-Lannes (2019) prove some results for unimodular lattices, which we generalize in the following.

Theorem 5.2 (A., Fretwell, Ingalls, Logan, Secord, Voight, 2022). *If $2 \mid k$, $\phi \in M(\Lambda)$ is an eigenform with $f = \theta^{(g)}(\phi) \neq 0$, If $2g < k$, then $c(\pi_\phi) = c(\pi_f \otimes \chi_{D^*}) \oplus [k-2g-1]$. If $k \leq 2g$, then $c(\pi_f \otimes \chi_{D^*}) = c(\pi_\phi) \oplus [2g-k]$.*

Consequently, e.g. when $2g < k$ one obtains

$$L(\phi, s) = L(\chi_{D^*} \otimes f, \mathrm{std}, s - \frac{k}{2} + 1) \cdot \prod_{i=g-\frac{k}{2}+1}^{\frac{k}{2}-1-g} \zeta(s + i - \frac{k}{2} + 1)$$

Example 5.3. If $g = 1$ and $f = \sum_{n=1}^{\infty} a_n q^n$, $T_p\phi = \lambda_p \phi$, then

$$\lambda_p = a_p^2 - \chi_{D^*}(p) p^{\frac{k}{2}-1} + p \cdot \frac{p^{k-3} - 1}{p - 1}$$

Example 5.4. If $\phi \in M(E_{16})$ as before, $g = 4$, then

$$c(\pi_\phi) = c(\tau)[4] \oplus [7] \oplus [1].$$

Recall $\phi = (286, -405)$, $e = (1, 1)$ so that $286e - \phi \equiv 0 \bmod 691$,

$$\lambda_p(e) = \frac{p^{15} - 1}{p - 1} + p^7 \quad c(\pi_e) = [15] \oplus [1]$$

As an application one can show Ramanujan's congruence that $\tau(p) \equiv p^{11} + 1 \bmod 691$.

This is a special case of a more general phenomenon of congruence between forms of different depths. Harder conjectured the recently proven analogue for Siegel modular forms of genus 2, namely

Theorem 5.5 (Harder's conjecture - Atobe, Chida, Ibukiyama, Katsurada, Ysmauchi 2023). *If $f \in S_{j+2k-2}(1)$ is an eigenform and $\mathfrak{q} \mid \frac{L(f,k+j)}{L(f,k+\frac{j}{2}+\epsilon}$ is a large enough prime of $\mathbb{Q}(f)$, then there exists a form $F \in S_{k,j}^{(2)}(1)$ s.t.*

$$\lambda_p(F) \equiv a_p(f) + p^{j+k-1} + p^{k-2} \pmod{\mathfrak{q}}'$$

for all p.

We show instances of an analogue with level in the setting of standard representations.

Theorem 5.6 (AFILSV 2022)**.** *Let* $f \in S_4(53, \chi_{53})$. *Then there exists* $F \in S_4^{(2)}(53, \chi_{53})$ *s.t.*

$$a_{1,p^2}(F) \equiv a_p(f)^2 - (1 + \chi_{53}(p)) \cdot p^3 + p^5 + p \pmod{\mathfrak{q}}$$

where $\mathfrak{q} \mid 397$ *is a prime in* $\mathbb{Q}(F)$.

This and other instances lead us to the following conjecture.

Conjecture 5.7. *Let* $f \in S_{j+k}(N, \chi)$ *and* $\mathfrak{q} \mid L_{\mathrm{alg}}(\mathrm{Sym}^2(f), j + 2k - 2)$*, then there exists* $F \in S_{k,j}(N, \chi)$ *and* $\mathfrak{q}' \mid \mathfrak{q}$ *such that*

$$a_{1,p^2}(F) \equiv a_p(f)^2 - \chi(p)p^{j+k-1} - p^{j+2k-5} + p^{j+2k-3} + p^{j+!} \pmod{\mathfrak{q})'$$

for all $p \nmid N$.

6. Summary

- Working explicitly with p-neighbors in $\mathrm{Cls}(\Lambda)$ we find systems of Hecke eigenvalues,
- Computational access to L-functions and Galois representations.
- Generalizes to other compact forms of reductive groups.
- The results inform us about the theory: Explicit description of images + phenomena encountered lead to more precise conjectures.