Some JMM Talks

Nir Elber

January 2025

Contents

1 Arithmetic Dynamics

This session happened on Wednesday the 8th of January. This session is an advertisement for an AIM workshop in November on dynamics of multiple maps.

1.1 Specializeations of Iterated Galois Groups of PCF Rational Functions

This talk was given by Jamie Juul. Throughout, k is a number field, $f \in k(x)$ is a polynomial of degree d, and we let $K_{\alpha,n}$ denote k adjoined with $f^{-n}(\alpha)$. We define $K_{\alpha,\infty}$ as the union and $G_{\alpha,n}$ as the Galois group; there are ways to guarantee that $K_{\alpha,n}/k$ is Galois. For transcedental t over k, one can do the same process, but we may write $K_n := K_{t,n}$ and $G_n := G_{n,t}$; to keep track of algebraicity, we will define $k_n := \overline{k} \cap K_n$.

One can think about t as a generic case: one can realize $G_{\alpha,\infty}$ inside G_∞ for any α. Thus, we are interested in when we get equality. For example, Hilbert's irreducibility theorem grants $[G_n : G_{\alpha,n}] = 1$ for generic α (depending on n); one expects $[G_\infty : G_{\alpha,\infty}] < \infty$ generically.

Note that f provides a natural tree structure to the set

$$\bigsqcup_{n\geq 0} f^{-n}(\alpha),$$

and $G_{\alpha,\infty}$ will permute the tree. This produces an "arboreal" Galois representation. One can check that this representation is injective by construction of $G_{\alpha,n}$ for each n. We remark that this grants an exact sequence

$$1 \to \mathrm{Gal}(K_\infty/k_\infty(t)) \to \mathrm{Gal}(K_\infty/k(t)) \to \mathrm{Gal}(k_\infty/k) \to 1,$$

where one can think about the left part as being transcendental/geometric and the right part as being algebraic.

We will look at the following class of functions.

Definition 1 (post-critically finite)**.** A map $f \in k(x)$ is *post-critcally finite* (PCF) if and only if each critical point is preperiodic.

And here are our theorems.

Theorem 2. Suppose $f \in k(x)$ is PCF and that $\operatorname{Gal}(K_1/k_1(t))$ is a p-group. Then there is $m(f,k) \geq 1$ such that $G_{\alpha,\infty} \cong G_\infty$ if and only if $G_{\alpha,m(f,k)} \cong G_m$.

Theorem 3. Choose $f(x) = x^{p^n} + c$ to be PCF, and let N be the size of the orbit of 0, and let k' be the compositum of degree p extensions of k_1 in k_∞. Then $G_{\alpha,\infty} \cong G_\infty$ if and only if $|\operatorname{Gal}(K_{\alpha,N}k'/k)| = |G_n|\,[k':k]$.

Morally, the second theorem is asking for some Galois group to be the correct size.

The key input is the following notion.

Definition 4 (Frattini)**.** Fix a profinite group G. Then the *Frattini subgroup* F is the intersection of all closed maximal subgroups.

So here is the sketch.

1. Because G_∞ is a profinite p-group, maximal subgroups have index equal to p and hence correspond to degree p extensions of $k(t)$.
2. Then one checks that there are only finitely many such extensions. Roughly speaking, one finds that $K_\infty\overline{k}$ has only finitely many extensions of $\overline{k}(t)$ of degree p and then specialize t. This uses the PCF assumption.
3. The point is that K_∞^F becomes some finite extensions of k and thus lives in some K_m. The result now follows with this m.

1.2 Profinite Iterated Monodromy Groups of PCF Unicritical Polynomials

This talk was given by Trevor Hyde.

We maintain the notation of the previous talk, though we let k be a general field and let $\widehat{k}$ be k_∞. Let ρ be the arboreal representation. We are intereseted in studying the group $\operatorname{Arb} = \rho(\operatorname{Gal}(\overline{k(y)}/k(y)))$; it may be helpful to understand $\overline{\operatorname{Arb}} = \rho(\operatorname{Gal}(\overline{k(y)}/\overline{k}(y)))$. It turns out that the short exact sequence

$$1 \to \overline{\operatorname{Arb}} \to \operatorname{Arb} \to \operatorname{Gal}(\widehat{k}/k) \to 1$$

splits, so it suffices to understand $\overline{\operatorname{Arb}}$, the extension $\widehat{k}/k$, adn the Galois action on $\overline{\operatorname{Arb}}$. The general expectation is that $\operatorname{Arb} = \overline{\operatorname{Arb}}$ is the full automorphism group of the tree; a special case to study is when f is PCF, and we frequently expect these equalities to fail; for example, in this case, $\overline{\operatorname{Arb}}$ is topologically finitely generated.

Remark 5. Richard Pink studied the case of $\deg f = 2$ in 2013. He found that $\overline{\operatorname{Arb}}$ only depends on some combinatorics having to do with f either being critically periodic or not. Further, he finds $\widehat{k} \subseteq k(\zeta_{2^\infty})$, with equality holding if f is critically periodic; else, $\widehat{k}/k$ is uniformly bounded (!) unless f is Chebychev.

Pink's work does a case-by-case analysis of the combinatorics, and it takes something like 90 pages. We are interested in higher-degree generalizations, which are potentially complicated. We specialize to unicritical polynomials to make the combinatorics as tractable as the quadratic case.

Theorem 6. Suppose $f(x) = x^d + c$ is unicritical (at 0) and PCF, and assume $\operatorname{char} k \nmid d$. Say that the orbit of 0 has n elements.

(a) There is an explicit recursive construction of $\overline{\operatorname{Arb}}$.

(b) If 0 is periodic, then $\overline{\operatorname{Arb}}$ only depends on n.

(c) If 0 is strictly preperiodic, then write $f^{m+1}(0) = f^{n+1}(0)$ for $m < n$ so that $f^n(0) = \zeta_d^\omega f^m(0)$ for some ω. Then $\overline{\operatorname{Arb}}$ only depends on (m, n, ω).

This ω is not seen in degree 2, and it says that the group depends not just on the pure tree combinatoris of 0.

Remark 7. Let's indicate some ideas of the proof. The post-critical combinatorics provide a recursive description of the conjugacy classes of the inertia subgroups. Then one shows some group-theoretic result that these conjugacy classes determine $\overline{\operatorname{Arb}}$ up to conjugacy.

Here are some applications.

- One can calculate the order of $\operatorname{Gal}(\overline{k}(f^{-\ell}(y))/\overline{k}(y))$ for all $\ell \geq 0$.
- One can compute $\overline{\operatorname{Arb}}^{\operatorname{ab}}$.
- Importantly, one can explicitly compute $\widehat{k}$. In particular, if f is a polynomial of degree d with $\operatorname{char} k \nmid d$, then $\widehat{k} \subseteq k(\zeta_{d^\infty})$. (The idea is to use the totally ramified point at $\infty \in \mathbb{P}^1_k$.)

For example, one has the following computations of $\widehat{k}$.

Theorem 8. Suppose $f(x) = x^d + c$ is unicritical (at 0) and PCF, and assume $\operatorname{char} k \nmid d$.

(a) If 0 is periodic, then $\widehat{k} = k(\zeta_{d^\infty})$.

(b) If 0 is strictly periodic, then either $d = 2$ and f is Chebychev, or $k(\zeta_d) \subseteq \widehat{k} \subseteq k(\zeta_{4d^2})$.

1.3 Square Patterns in Dynamical Orbits

This talk was given by Vefa Goksel. For now, K is a field, and $f \in K[x]$ of degree $d \geq 2$. For $a \in K$, we let $\mathcal{O}_f(a)$ denote the forward orbit. We are interested in the following two notions.

Definition 9. Choose $f \in K[x]$ of degree $d \geq 2$. Then f is *dstable* if and only if f^n is irreducible over K for all $n \geq 1$. We say f is *eventually stable* if and only if the number of irreducible factors of f^n is bounded as $n \to \infty$.

If K is global, one expects stability to be generic. We will be interested in the case where K is finite, where these notions are rare. For example, one has the following.

Lemma 10 (Boston–Jones). Let $\mathbb{F}_q$ be a finite field with q odd, and let $f \in \mathbb{F}_q[x]$ be monic and quadratic with critical point γ. Then f is stable if and only if the set

$$\{-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots\}$$

has no squares.

Lemma 11 (Ostafe–Shparlinski). Let $\mathbb{F}_q$ be a finite field with q odd, and let $f \in \mathbb{F}_q[x]$ be monic and quadratic with critical point γ. Then $\#\mathcal{O}_f(\gamma)$ is $O(q^{3/4})$.

The second lemma is shown by doing some character summing of $\chi(f^i(\gamma))$, where $\chi\colon \mathbb{F}_q^\times \to \mathbb{C}^\times$ is the nontrivial quadratic character. We are interested in improving some of these character sums. Let's add some hypotheses.

Definition 12. A polynomial f is *dynamically ordinary* if and only if each n has an irreducible factor g_n of f^n not found in any prior $f^\bullet$. We say that f is *dynamically* 2*-ordinary* if and only if there is such a g_n with odd multiplicity.

There is a classification of such dynamically ordinary polynomials.

Proposition 13. Choose f as above. Then f is not dynamically ordinary if and only if f takes the form $f(x) = A(x-B)^{p^e}$.

There is also a rather more complicated classification of dynamically 2-ordinary polynomials.

Anyway, here is our main result.

Theorem 14. Fix an odd prime power q, and choose $f \in \mathbb{F}_q[x]$ to be dynamically 2-ordinary of degree d. For $a \in \mathbb{F}_q$, suppose the sequence $\{\chi(f^\bullet(a))\}$ is periodic of period m. Then $\#\mathcal{O}_f(a)$ is $O\left(mq^{\frac{2\log_2 d+1}{2\log_2 d+1}}\right)$.

The idea is to expand out $\#\mathcal{O}_f(a)$ as some character sum and then bound it using the Weil conjectures. Note being dynamically 2-ordinary comes in because the Weil conjectures require some smoothness assumption on a product of some $f^\bullet$s; in particular, one needs to know this product is non-square, which is where the odd multiplicity requirement comes from.

1.4 Bad Reduction of PCF Maps

This talk was given by Patrick Ingram. There is an analogy between elliptic curves with complex multiplication and PCF maps. Let E be an elliptic curve over a number field K, and choose a prime $\mathfrak{p}$. Having good reduction at $\mathfrak{p}$ means that E has an integral model over $\mathcal{O}_\mathfrak{p}$, which grants an elliptic curve over $\mathbb{F}_\mathfrak{p}$. Sometimes having good reduction is not possible over K, so we recall that having potentially good reduction means that E has good reduction after extending the field. We now recall the following.

Theorem 15. Choose an elliptic curve E with complex multiplication. Then E has potentially good reduction everywhere.

One can show this for elliptic curves by instead showing $j(E)$ is an algebraic integer.

We now return to dynamics. A rational map $f \in K(x)$ has good reduction at $\mathfrak{p}$ if and only if it can be written in homogeneous coordinates as $f(X,Y) = [A(X,Y) : B(X,Y)]$ for polynomials A and B in $K_\mathfrak{p}$, and it has potential good reduction if one can change variables to get good reduction. For example, one can check that unicritical PCF polynomials have potentially good reduction everywhere. Let's give a quick criterion.

Lemma 16. Choose z such that $f^k(z) = z$. If f has potentially good reduction at $\mathfrak{p}$, then $\left|(f^k)'(z)\right|_\mathfrak{p} \le 1$.

Dynamically, this says that there are no "repelling" cycles.

We are interested in knowing what sort of reductions we can get uniform in the degree d of f. Explicitly, this comes down to constructing some poorly behaved polynomials with repelling cycles at $\mathfrak{p}$. For polynomials, this is folklore.

Proposition 17. A PCF polynomial f over $\mathbb{Q}$ of degree d has potentially good reduction for all $p \geq d$.

We would like to improve this. For example, there is also a lower bound.

Proposition 18. For each prime $p < d$ with $p \nmid d$, there are infinitely many PCF polynomials f of degree d with a p-adically repelling fixed point.

Recall that having a p-adically repelling fixed point then means it does not even have potentially good reduction. The idea is to consider the family

$$f(x) = pz^d - dt^{d-p}x^p$$

as t varies. One finds that f is PCF if and only if t is preperiodic. One can then solve $f^2(t) = 0$ to find a working t.

Remark 19. In some sense, what is happening is that PCF polynomials are "special points" in our one-parameter family of polynomials.

The rest of the talk returned to rational functions. Here is the main result.

Theorem 20. Choose $d \geq 2$ and $p \nmid d(d-1)$. Then there is a PCF rational function of degree d with a fixed point which repelling at some prime above p.

One shows this again by choosing a one-parameter family carefully.

1.5 Necklaces, Permutations, and Periodic Critical Orbits for Quadratics

This talk was given by Andrea Chen, Sophi Lie, Matthew Qian, and Leonna Wang; they are a team of high schoolers who did work in the PROMYS program under Matt Baker.

We abandon the existing notation.

Definition 21. Let G_n denote the nth Gleason polynomial, whose roots are the $c \in \mathbb{C}$ such that 0 is a critical point of exactly period n under the iteration $z \mapsto z^2 + c$.

This can be computed recursively by computing iterates of $z \mapsto z^2 + c$ and then dividing out by the previous Gleason polynomials. It is conjectured that G_n is irreducible. Here is some analogous result.

Theorem 22 (Buff–Floyd–Koch–Parry)**.** The number of irreducible factors of $G_n \pmod 2$ equals the number of real roots of G_n.

The given proof is done be an explicit computation: one finds that this quantity is

$$\frac{1}{2n} \sum_{\substack{m \mid n \\ m \text{ odd}}} \mu(m) 2^{m/n}.$$

We are interested in giving a combinatorial proof of the result.

Here are some definitions from combinatorics.

Definition 23. A permutation is *unimodal* if and only if its graph is decreasing and then increasing.

Definition 24. A binary necklace of length n is a sequence of n bits, considered up to cyclic permutation.

We now give the main theorem.

Theorem 25. Fix n. Then we give explicit bijections for the following sets.

(i) Real roots of G_n.

(ii) Irreducible factors of $G_n \pmod 2$.

(iii) The set of cyclic unimodal permutations.

(iv) Binary necklaces of length n with an even number of 1s.

(v) Binary necklaces of length n with an odd number of 1s.

Let's list some inputs.

- Teichmuller dynamics grants bijections between (i) and (iii).
- Galois theory can give a bijection between (ii) and some special set ofbinary necklaces.
- Symbolic dynamics can then give a bijection between cyclic unimodal permutations and the above sets of binary neckalces in (iv) and (v).
- Lastly, one does some explicit combinatorics with binary necklaces for a little correction.

1.6 Local Fields, Iterated Extensions, and Julia Sets

This talk was given by Donald Lee.

Let K be a local field with disctete valuation ν, and we let p be the residue characteristic. We are interested in iterates of the polynomial $f(z) = z^\ell - c$. If $\deg f = p$, then one finds that the field extensions of the solutions $f^n(z) = \alpha$ (as $\alpha \in K$ varies) is bounded if $\nu(c) < -p/(p-1)$ and infinite otherwise, and one can say something about the ramification in the latter case. This is shown by a study of the underlying arboreal Galois representation.

We show analogous results for ℓ a power of p with $p/(p-1)$. We will use some theory about Berkovich spaces. Let $\mathbb{P}^1_{\text{an}}$ be the Berkovich projective line, which is the Hausdorff compactification of $\mathbb{P}^1(\mathbb{C}_p)$. Roughly speaking, one adds "generic" points to $\mathbb{P}^1(\mathbb{C}_p)$ to fix the totally disconnected topology. One is now able to define a (filled) Berkovich Julia set attached to f in the usual way by asking for iterates of f to not escape to ∞; we let $\mathcal{J}_f$ denote the boundary, and it is the Berkovich Julia set. Here is our main result.

Theorem 26. Write $\ell = p^k$ for $c \in \overline{\mathbb{Q}_p}$, and set $\nu_\infty = -\ell/(\ell-1)\nu(\ell)$.

(a) If $\nu(c) < \nu_\infty$, then $\mathcal{J}_f$ is a Cantor set of points in $\mathbb{P}^1(\mathbb{C}_p)$.

(b) Otherwise, $\mathcal{J}_f$ has non-generic points.

One can even more precisely study the non-generic points, though one needs another cutoff ν_{good} to keep track of f having good reduction. Do note that one needs a finer understanding of the points of $\mathbb{P}^1_{\text{an}}$ for these descriptions than we have given here. Roughly speaking, one uses the Newton polygon to do the computation of the filled Julia set.

Here is our result on the field extensions.

Theorem 27. Suppose $p \nmid \ell$ and $\ell > 0$. Then the field extensions generated by the solutions to $f^n(z) = \alpha$ (for $\alpha \in K$) are bounded for small $\nu(c)$ and infinitely wildly ramified for large $\nu(c)$.

The idea is to use Krasner's lemma to do the bounding. For example, for small $\nu(c)$, one shows that n large enough has all the solutions to $f^{n+1}(z) = \alpha$ too close to the solutions to $f^n(z) = \alpha$, showing boundedness.

1.7 Arithmetic Dynamics on Character Varieties

This talk was given by Cigole Thomas.

Let's begin with a short introduction to character varieties. There is a topological ingredient, which is a finitely presented group Γ, which can be thought of as a fundamental group. Then there is a geometric component G, which is a complex reductive algebraic group.

Example 28. Consider $\Gamma = \mathbb{Z}^2$ and $G = \mathrm{SL}_n(\mathbb{C})$.

Letting r be the number of generators of Γ, then there is an embedding $\mathrm{Hom}(\Gamma, G) \hookrightarrow G^r$. But note that G acts on $\mathrm{Hom}(\Gamma, G)$ by conjugation, and we let the character variety $\mathfrak{X}$ be the quotient. To make the quotient $\mathfrak{X}$ behave, one should correct the space a bit.

We remark that one can also take $\mathbb{F}_q$-points.

Example 29. One can compute $\mathrm{Hom}(\mathbb{Z}^2, \mathrm{SL}_n(\mathbb{F}_q))$ is in bijection with pairs (A, B) of commuting matrices, and after ridding of the conjugation action and correcting the quotient, we find that we are talking about sets of pairs simultaneously diagonalizable matrices.

Note that $\mathrm{Aut}(\Gamma)$ acts on $\mathrm{Hom}(\Gamma, G)$ by precomposition. By taking the quotient, we see that $\mathrm{Out}(G)$ acts on $\mathfrak{X}$; we are interested in this second action.

Example 30. Note $\mathrm{Aut}(\mathbb{Z}^2) = \mathrm{GL}_2(\mathbb{Z})$, so the above defines a homomorphism $\mathrm{GL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathfrak{X})$ which is essentially given by matrix multiplication.

This action turns out to not be transitive in general, so perhaps one can try to recover a result in the large q limit. And in absence of transitivity, maybe we can ask for a large orbit. For example, one can ask when the limit

$$\lim_{p\to\infty} \frac{\max\{|\mathrm{Orb}(v)| : v \in X\}}{|X|}$$

equals 1. Roughly speaking, this is a finite-field analogue of ergodicity.

Let's work with the running example. Here is a strategy for the computation.

1. Stratify the space of pairs of matrices depending on eigenvalues.
2. Then count the number of points in each stratum.
3. Now, each stratum actually has a subgroup of $\mathrm{SL}_2(\mathbb{F}_p)^2$ containing the orbit.
4. The previous step allows one to say something about the orbit.

This gives a main theorem.

Theorem 31. With $\Gamma = \mathbb{Z}^2$ and $G = \mathrm{SL}_2(\mathbb{F}_q)$, one has

$$\lim_{p\to\infty} \frac{\max\{|\mathrm{Orb}(v)| : v \in X\}}{|X|} = \frac{1}{2}.$$

There are generalizations to $\Gamma = \mathbb{Z}^r$ and even $\mathrm{SL}_3(\mathbb{F}_q)$, but the computations become intractable in large rank.

1.8 Ramified Approximation and Semistable Reduction

This talk was given by Xander Faber. For now, K is a nonarchimedean local field with valuation v, and π is a uniformizer. As usual, $\mathcal{O}_K$ is the valaution ring, $\widetilde{K}$ is the residue field with characteristic $p > 0$, K_s is a separable closure (which has an induced valuation v). Then $\mathbb{C}_K$ is the completion of K_s, and we let G_K be its Galois group.

This talk is interested in (closed) disks $D(a,r)$ in $\mathbb{C}_K$. Note that a G_K-invariant disk $D(a,k)$ will contain all the roots of some polynomial f; in fact, one can check that this is an equivalence. Roughly speaking, given a G_K-invariant disk $D(a,r)$, one can ask for the minimum degree of an algebraic element in $D(a,r)$ and how to find them. Of course, one can take the degree of a and r to produce a minimal degree, but maybe there are better ones.

Here is an example result.

Proposition 32. Fix a G_K-invariant disk D. If D contains an element $a \in K_s$ with degree coprime to p, then $D \cap K \neq \varnothing$.

Proof. Well, given algebraic $a \in D$, one just takes $\frac{1}{\deg \alpha} \operatorname{tr} a \in D \cap K$, which is a legal quotient because $\deg \alpha$ is coprime to p. ■

Here is an extension.

Lemma 33 (Ax)**.** Fix a G_K-invariant disk D. If D contains an element $a \in K_s$ of degree p^m (where $p \nmid m$), then D contains an element of degree dividing p^e.

The idea is to consider some power series expansion of $f(a+t)$ where f is the minimal polynomial, and one hopes to find the element at small t.

There are results like this. Here is another.

Proposition 34. Let D be a G_K-invariant disk. If D contains an elment $a \in K_s$ which generates an unramified extension of K, then $D \cap K \neq \varnothing$.

In total, one may hope to descend algebraic elements of Galois-invariant disks along totally tamely ramified extensions and even unramified extensions. One can even descend to a p-extension using Ax's lemma. Thus, we hope that we can go down to a totally wildly ramified extension. However, the kind of reduction we are hoping for is backward: the order of fields from K to L is in general unramified then tamely ramified then wildly ramified.

However, we are still able to recover some kind of result, which is our main theorem.

Theorem 35. Suppose D is a disk containing all conjugates of some β. Then there is an explicit $\alpha \in D \cap K_s$ such that $K(\alpha)/K$ is separable and totally wildly ramified.

Let's give a dynamical application. Fix $f\colon \mathbb{P}^1_K \to \mathbb{P}^1_K$ of degree $d \geq 2$, and we recall that we can write $f(X,Y) = [F(X,Y) : G(X,Y)]$. We say that f has good reduction if and only if its reduction to $\widetilde{K}$ has the same degree as f.

Theorem 36. Fix $f\colon \mathbb{P}^1_K \to \mathbb{P}^1_K$ of degree at least 2. Then f has good reduction if and only if $\operatorname{ordRes}(f) = 0$.

Here, ordRes has to do with the order of the homogeneous coordinates F and G.

Now let's give an application from arithmetic geometry.

Theorem 37. An elliptic curve E with potentially good reduction achieves good reduction after base-change by a totally ramified extension.

2 Cohomology of Arithmetic Groups

These talks happened on Wednesday the 8th of January.

2.1 Hyperelliptic Curves, the Scanning Map, and Moments of L-Functions

This talk was given by Craig Christopher Westerland. Given a squarefree positive integer d, we let χ_d denote the Kronecker symbol: for primes p, we have $\chi_d(p) = \left(\frac{p}{d}\right)$ and then extend multiplicatively. (There is some definition at $p = 2$ which is not complicated, but we will not elaborate on it.) There is an L-function

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for any Dirichlet character χ. There is an Euler product, meromorphic continuation, and functional equation for $L(s, \chi)$, and there is an expected Riemann hypothesis. One may be interested in the moments

$$M_r(D) := \sum_{\substack{|d|<D \\ d \text{ squarefree}}} L(1/2, \chi_d)^r$$

as $r \geq 0$ varies. The value of $L(1/2, \chi_d)$ is potentially interesting for functional equation reasons. One has the following conjecture, which comes from some conjectures in random matrix theory.

Conjecture 38. We have $M_r(D) \sim DQ_r(\log D)$, where Q_r is some explicit polynomial of degree $r(r+1)/2$.

Remark 39. We remark that there is also a conjecture on moments of $\zeta\left(\frac{1}{2} + it\right)$. Explicitly, one expects

$$\int_0^T \left|\zeta\left(\frac{1}{2} + it\right)\right|^{2r} dt \sim C_r T (\log T)^{r^2}$$

for an explicit constant C_r. One only knows $r \in \{1, 2\}$, and they are about a hundred years old.

We will study some related L-functions coming from algebraic geometry via the function field analogy. Using the same notions of quadratic residues, one can define Dirichlet characters (and the Kroneckedr symbol) on $\mathbb{F}_q[t]$, and we produce an L-function defined exactly analogously as

$$L(s, \chi) = \sum_{\substack{f \in \mathbb{F}_q[x] \\ f \text{ monic}}} \frac{\chi(f)}{|f|^s},$$

where $|f|$ is $\#\mathbb{F}_q[t]/(f) = q^{\deg f}$. (The reason for taking monic polynomials is that it is actually more natural to sum over ideals than elements.) There is still an Euler product, meromorphic continuation, and functional equation.

Now, here is our main result on moments.

Theorem 40. Let q be an odd prime power. Then

$$\frac{1}{q^{2g+1}} \sum_{\substack{d \text{ squarefree} \\ \deg d = 2g+1}} L(1/2, \chi_d)^r = Q_r(2g+1) + O\left(4^{g(r+1)} q^{-g/12}\right)$$

for some explicit polynomial Q_r of degree $r(r+1)/2$.

We remark that one needs $q > 4^{12(r+1)}$ for the error term to not overwhelm the main term. Let's sketch the ideas.

- One can interpret the left-hand side as counting $\mathbb{F}_q$-points on a configuration space $\operatorname{Conf}_{2g+1}$.
- The Weil conjectures then relate point-counts to cohomology.

- Lastly, one uses homotopy theory to compute the cohomology.

Let's recall the definition of Conf.

Definition 41. For a ring R and $n \geq 0$, we define the *configuration sheaf* $\mathrm{Conf}_n(R)$ as the set of monic squarefree polynomials d of degree n. We then define the *Braid group* as $B_n := \pi_1 \mathrm{Conf}_n(\mathbb{C})$.

Remark 42. When R is an algebraically closed field, then we are indeed looking at the set of n-tuples $(z_1, \ldots, z_n)$ of distinct points, taken up to permutation.

Now, to access $L(1/2, \chi_d)$, one uses hyperelliptic curves.

Theorem 43. Choose a monic squarefree polynomial $d \in \mathbb{F}_q[x]$. Then we let $C_d \subseteq \mathbb{P}^2$ be the hyperelliptic curve with affine model $y^2 = d(x)$. Then

$$L(1/2, \chi_d) = \mathrm{tr}\left(\mathrm{Frob}_q | \wedge^\bullet \mathrm{H}^1_{\text{ét}}(C_d)\right).$$

One has to do some work to go from $L(s, \chi_d)$ to ζ_{C_d}, and then the Weil conjectures explain how to talk about ζ_{C_d}.

Thus, we now see that we are interested in studying

$$\frac{1}{q^{2g+1}} \sum_{d \in \mathrm{Conf}_{2g+1}(\mathbb{F}_q)} \mathrm{tr}\left(\mathrm{Frob}_q | \wedge^\bullet \mathrm{H}^1_{\text{ét}}(C_d)\right).$$

We now recall the Grothendieck–Lefschetz trace formula, which gives

$$\sum_{x \in X(\mathbb{F}_q)} \mathrm{tr}(\mathrm{Frob}_q | \mathcal{L}_x) = \sum_{k=0}^{2\dim X} (-1)^k \,\mathrm{tr}\left(\mathrm{Frob}_q | \mathrm{H}^k_{\text{ét}}(X, \mathcal{L})\right)$$

for a local system $\mathcal{L}$ on X. Thus, we see that we are interested in computing the cohomology

$$\mathrm{H}^k_{\text{ét}}\left(\mathrm{Conf}_{2g+1}, (\wedge^\bullet V)^{\otimes r}\right),$$

where V is the local system $d \mapsto \mathrm{H}^1_{\text{ét}}(C_d, \mathbb{F}_q)$. One finds that V is the reduced Burau representation of the Braid group B_{2g+1}, and it can be computed with explicitly.

Now, the idea is to decompose $(\wedge^\bullet V)^{\otimes r}$ into irreducible representations of $\mathrm{Sp}_{2g}(\mathbb{Z})$ named V_λ. (The symplectic structure comes from the curve C_d.) One finds that the multiplicities are some explicit polynomials in r of degree $r(r+1)/2$. It now turns out that there is some uniform homological stability.

Theorem 44. Choose $k < g/12$. Then

$$\mathrm{H}^k(\mathrm{Conf}_{2g-1}(\mathbb{C}), V_\lambda) \cong \mathrm{H}^k(\mathrm{Conf}_{2g+1}(\mathbb{C}), V_\lambda).$$

What is remarkable is that the stability region $k < g/6$ does not depend on λ (or in particular r)! The moral of the story is that we are allowed to tend g large, which can be computed.

Theorem 45. One can compute a generating function for

$$\lim_{g \to \infty} \mathrm{H}^*(\mathrm{Conf}_{2g-1}(\mathbb{C}), V_\lambda),$$

along with an action of Frob_q.

Note we are allowed to work over $\mathbb{C}$ mostly because of the available comparison theorems.

Let's explain the second theorem a little. Given a based $(\mathbb{Z}/2\mathbb{Z})$-space, one can define $\mathcal{H}_g(X)$ as consisting of pairs (d, f) where $d \in \mathrm{Conf}_{2g+1}(\mathbb{C})$ and f is some $(\mathbb{Z}/2\mathbb{Z})$-equivariant map $C_d/\iota \to X$. For partition λ, we let S^λ denote the corresponding Schur functor, and one finds that

$$\mathrm{H}_*(\mathcal{H}_g(K(A))) = \bigoplus_\lambda S^\lambda(A) \otimes \mathrm{H}_*(B_{2g+1}, S^\lambda(V))$$

for any graded $\mathbb{Q}$-algebra A. We are interested in the right-hand homology groups, so it will be enough to let A vary so that we can solve out the coefficients $S^\lambda(A)$. Then eventually one can compute $\mathrm{H}_*(\mathcal{H}_g(K(A)))$ with large g using homotopy theory. One can compute the Galois action by tracking through the computation and being careful with comparisons.

2.2 Uniform Twisted Homological Stability

Jeremy Miller gave this talk. The goal of this talk is to prove the homological stability discussed in the previous talk. Here is the most basic case of homological stability, shown by an explicit computation of group homology groups.

Theorem 46 (Nakoaka)**.** For $i \le n/2$, there are isomorphisms $\mathrm{H}_i(S_n, \mathbb{Z}) \to \mathrm{H}_i(S_{n+1}, \mathbb{Z})$.

For twisted homological stability, we want to also want to change the coefficients in n. Then one has the following

Theorem 47. Let S_n act on $\mathbb{Z}^n$ by permuting the coordinates. For $i \le n/2$, there are isomorphisms $\mathrm{H}_i(S_n, \mathbb{Z}^n) \to \mathrm{H}_i\left(S_{n+1}, \mathbb{Z}^{n+1}\right)$ is an isomorphism for $i \le (n-1)/2$.

Proof. Shapiro's lemma gives $\mathrm{H}_i(S_n, \mathbb{Z}^n) = \mathrm{H}_i(S_{n-1})$. ■

The moral of the story is that twisting homological stability may make the stability range "worse."

For our application, we have the following situation. Given a partition λ of length at most g, we can produce (bijectively) irreducible algebraic Sp_{2g} named $V_\lambda(g)$. Then there is a Burau representation $B_{2g+1} \to \mathrm{Sp}_{2g}(\mathbb{Z})$, so one can state and prove a stability result.

Theorem 48. There is an isomorphism $\mathrm{H}_i(B_{2g+1}, V_\lambda(g)) \to \mathrm{H}_i(B_{2g+1}, V_\lambda(g+1))$ is an isomorphism for $i \le g - |\lambda|$.

Our main result is the following.

Theorem 49. There is an isomorphism $\mathrm{H}_i(B_{2g+1}, V_\lambda(g)) \to \mathrm{H}_i(B_{2g+1}, V_\lambda(g+1))$ is an isomorphism for $i \le g/12$.

The point is that we have removed a dependence on λ. The same technique works for mapping class groups instead of the Braid group. We do remark that it is known to Borel that there is twisted homological stability for $i \le g/4$ for the group $\mathrm{Sp}_{2g}(\mathbb{Z})$.

Let's say something about the proof in the case of mapping class groups. Let R be the disjoint union of the classifying spaces $\mathrm{BMod}_{g,1}$. This is a monoid where taking "pairs of pants" forms the required product. Similarly, define A as the disjoint union of the classifying spaces $\mathrm{BSp}_{2g}(\mathbb{Z})$, which is again a monoid, and the Torelli map provides a map $R \to A$. Now, A "has" twisted uniform homological stability, and we would like the same to be true for R. Roughly speaking, this turns into a homological algebra exercise. The main input is that "derived R-module generators" of A/R have a vanishing line, and the vanishing line comes from some connectivity input from topology.

2.3 Hopf Algebras and the Cohomology of $\mathrm{GL}_n(\mathbb{Z})$

This talk was given by Peter Patzt. Our goal is to compute $\mathrm{H}^k(\mathrm{SL}_n(\mathbb{Z}), \mathbb{Q})$. We will state computational results for $n \leq 7$. There are many 0s. For example, one has the following.

Theorem 50 (Borel–Serre)**.** We have $\mathrm{H}^k(\mathrm{SL}_n(\mathbb{Z}), \mathbb{Q}) = 0$ for $k > \binom{n}{2}$.

In fact, it is conjectured that the cohomology vanishes for $k > \binom{n-1}{2}$. One can state this equivalently as $\mathrm{H}^{\binom{n}{2}-i}(\mathrm{SL}_n(\mathbb{Z}), \mathbb{Q}) = 0$ for $i \leq n-2$. This has been proven in a few cases.

One also knows quite a bit about $i \leq n-2$.

Theorem 51 (Borel)**.** For $k \leq n-2$, we have

$$\mathrm{H}^k(\mathrm{SL}_n(\mathbb{Z}), \mathbb{Q}) \cong \bigwedge^k \langle \sigma_5, \sigma_9, \sigma_{13}, \ldots \rangle.$$

This still leaves quite a bit to compute, which is "unstable." For example, sometimes one can pull back a $\sigma_\bullet$ as above to the unstable range, but there is still something to compute. For example, $\mathrm{H}^3(\mathrm{SL}_4(\mathbb{Z}), \mathbb{Q}) = \mathbb{Q}$, but this class is not explained by one of the "stable" $\sigma_\bullet$ classes.

Here is our first result.

Theorem 52. There is a graded commutative algebra structure on $\bigoplus_{k,n} \mathrm{H}^k(\mathrm{SL}_n(\mathbb{Z}), \mathbb{Q})$ with the graded multiplication looking like

$$\mathrm{H}^{\binom{n}{2}-k}(\mathrm{SL}_n(\mathbb{Z}), \mathbb{Q}) \otimes \mathrm{H}^{\binom{n}{2}-\ell}(\mathrm{SL}_m(\mathbb{Z}), \mathbb{Q}) \to \mathrm{H}^{\binom{m+n}{2}-(k+\ell)}(\mathrm{SL}_{m+n}(\mathbb{Z}), \mathbb{Q}).$$

For example, we now find that we can divide the algebra into even and odd parts named $\mathrm{H}^{\mathrm{odd}}$ and $\mathrm{H}^{\mathrm{even}}$ respectively. The graded pieces $\mathrm{H}^\bullet_{k,n}$ correspond to some cohomology of $\mathrm{GL}_n(\mathbb{Z})$. Now, here is our second main result.

Theorem 53. One has that $\mathrm{H}^{\mathrm{odd}}$ is a free graded commutative algebra.

In particular, one finds that products explain some classes seen in our cohomology after combining some easy-to-find classes (from H^0) with the known stability classes.

Analogous to the odd case, we have our third main result.

Theorem 54. One has that $\mathrm{H}^{\mathrm{even}}$ is a free graded commutative algebra.

Once again, there are the stable classes and a class from H^0, and all the known unstable classes are found as products.

Let's say something about how the last two theorems are proved. The key input is from Hopf algebras.

Theorem 55 (Leray)**.** A graded commutative $\mathbb{Q}$-Hopf algebra with constants $\mathbb{Q}$ is free graded commutative.

Thus, the point is to find a Hopf algebra structure on $\mathrm{H}^{\mathrm{even}}$ and $\mathrm{H}^{\mathrm{odd}}$.

2.4 The Cohen–Lenstra Moments over Function Fields

This talk was given by Aaron Landesman. Let's begin by reviewing the Cohen–Lenstra heuristics. We are interested in the ℓ-torsion of class groups of imaginary quadratic number rings for fixed prime ℓ.

Conjecture 56 (Cohen–Lenstra)**.** Fix a prime-power q. For odd prime ℓ, one has

$$\lim_{X\to\infty} \mathbb{E}_{K \text{ imag. quad.}} \# \operatorname{Cl}(\mathcal{O}_K)[\ell] = 2.$$

Only $\ell = 3$ is known. For function fields, we work with the space $\mathcal{MH}_{n,q}$ of function fields K of monic hyperelliptic curves $y^2 = f(t)$, and we let $\mathcal{O}_K$. The following has been known.

Theorem 57. For odd prime ℓ such that $\gcd(\ell, q(q-1)) = 1$, one has

$$\lim_{q\to\infty} \lim_{\substack{n\to\infty \\ n \text{ odd}}} \mathbb{E}_{K\in\mathcal{MH}_{n,q}} \# \operatorname{Cl}(\mathcal{O}_K)[\ell] = 2.$$

We will show the equality for large q, effectively removing the limit. Thus, we find that we are interested in some point-counts over $\mathbb{F}_q$, from which one can use some algebriac geometry. Here is our space.

Definition 58 (Hurwitz space)**.** Fix a group G and a conjugacy class c. Then we define the *Hurwitz space* $\operatorname{Hur}_n^{G,c}$ as the space of Galois G-covers $X \to \mathbb{A}^1$ branched over n points with inertia contained in c.

Then order-ℓ elements in class groups correspond to $\operatorname{Hur}_n^{G,c}$. We take a moment to note that taking the branched locus produces a map $\operatorname{Hur}_n^{G,c} \to \operatorname{Conf}_n$. Here is our key input.

Theorem 59. Choose an odd prime ℓ and $c \subseteq D_{2\ell}$ the conjugacy classes of reflections. For large n, there is an isomorphism

$$\mathrm{H}_i(Z, \mathbb{Q}) \to \mathrm{H}_i(\operatorname{Conf}_n, \mathbb{Q}),$$

for any component $Z \subseteq \operatorname{Hur}_n^{D_{2\ell},c}$.

For a taster, consider $\ell = 3$ so that $G = S_3$; say $c = \{x, y, z\}$, which are the three transpositions. We would like a stability result for the map $\operatorname{Hur}^c \to \operatorname{Conf}^c$, where

$$\operatorname{Hur}^c := \bigsqcup_{n\ge 0} \operatorname{Hur}_n^{S_3,c},$$

$$\operatorname{Conf}^c := \bigsqcup_{n\ge 0} \bigsqcup_{\pi_0(\operatorname{Hur}_n^c} \operatorname{Conf}_n.$$

The stability result comes from descent, and it uses some homotopy theory.

Remark 60. One can hope to prove more than just for dihedral groups. This becomes related to Malle's conjecture in arithmetic statistics.

2.5 Moduli of Stable Elliptic Curves in $\mathbb{P}^r$

This talk was given by Siddarth Kannan.

We define $\mathcal{M}_{g,n}(\mathbb{P}^r, d)$ consisting of a smooth proper curve C of genus g with n distinct marked points such that there is an embedding $f\colon C \to \mathbb{P}^n$ such that $f_*[C] = d[\mathcal{O}(1)]$, taken up to isomorphism. One can compactify this space by replacing C with connected nodal curves, and the marked points are chosen to be smooth.

Remark 61. Let's give a few reasons to care.

- The Gromov–Witten invariants of $\mathbb{P}^r$, which are symplectic invariants of $\mathbb{P}^r$, can be seen as intersection numbers on $\overline{\mathcal{M}}_{g,n}(\mathbb{P}^r, d)$.

- Brill–Noether theory has to do with the map $\mathcal{M}_{g,n}(\mathbb{P}^r, d) \to \mathcal{M}_{g,n}$.

We would like to understand the rational cohomology of our moduli space. Note that these are representations of S_n via the action on the marked points. For a taste of the difficulty, we note that $g > 0$ makes $\mathcal{M}_{g,n}(\mathbb{P}^r, d)$ is not dense in $\overline{\mathcal{M}}_{g,n}(\mathbb{P}^r, d)$ and is highly singular. On the other hand, much is known for $g = 0$ because this compactification is much better-behaved. There is also much known for $d = 0$ because then we are looking at $\mathcal{M}_{g,n}$. Otherwise, not much is known.

Theorem 62. For fixed i, g, r, and d, the group $\mathrm{H}_i(\overline{\mathcal{M}}_{g,n}(\mathbb{P}^r, d), \mathbb{Q})$ stabilizes.

Today we will talk about $g = 1$. In particular, we will compute the S_n-invariant Euler characteristic of $\overline{\mathcal{M}}_{g,n}(\mathbb{P}^r, d)$. Explicitly, χ^{S_n} of a variety X with S_n-action, we define $\chi^{S_n}(X)$ as the Euler characteristic in the Grothendieck ring of S_n-representations. Explicitly,

$$\chi^{S_n}(X) = \sum_{i=0}^{\infty} (-1)^i [\mathrm{H}_c^i(X, \mathbb{Q})],$$

where we view the cohomology $\mathrm{H}_c^i(X, \mathbb{Q})$ as a representation of S_n. We may write χ_λ for the multiplicity of the Specht module V_λ. For example, we are able to state the following result.

Theorem 63. Fix $n, d \geq 0$. For each partition λ of n, there are functions $a_1^\lambda, \ldots, a_{d+1}^\lambda \colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}$ such that

$$\chi_\lambda(\overline{\mathcal{M}}_{g,n}(\mathbb{P}^r, d)) = a_1^\lambda(g)\binom{r+1}{1} + \cdots + a_{d+1}^\lambda(g)\binom{r+1}{d+1}.$$

The moral of the story is that we can write the Euler characteristic out in terms of certain binomial coefficients. Roughly speaking, by working over $\mathbb{C}$, one is eventually able to turn this into combinatorics. From here, one is able to compute a generating function; it turns into some graph enumeration.

2.6 Tropicalizations of Locally Symmetric Spaces

This talk was given by Juliette Bruce.

Let's begin with a quick summary of our picture. Curves have a moduli space $\mathcal{M}_g$ with compactification $\overline{\mathcal{M}}_g$ with boundary understood by some stable graphs, which then have attached some "tropical" combinatorial gadgets; there is also a chain complex to compute its homology. Then abelian varieties also have a moduli space $\mathcal{A}_g$ with a compactification $\overline{\mathcal{A}}_g^\Sigma$ whose boundary is described combinatorially via perfect cones, which then have attached some "tropical" combinatorial interpretation; it turns out that one still has a chain complex. One may hope to generalize from $\mathcal{A}_g$ to generally locally symmetric spaces $\Gamma \backslash D$ where D is a Hermitian symmetric domain and Γ is an arithmetic group.

So let's begin with curves. For any variety X, it turns out that there is a subspace $W_0\mathrm{H}_c^i(X, \mathbb{Q})$ of $\mathrm{H}_c^i(X, \mathbb{Q})$ which "comes from" combinatorics. Namely, given a simple normal crossings compactification $\overline{X}$ of X, then the subspace explains what the boundary looks like. This gives the following result.

Theorem 64 (Chan–Golatius–Payne)**.** For $g \geq 1$, there is an isomorphism

$$W_0\mathrm{H}_c^*(\mathcal{M}_g, \mathbb{Q}) \cong \mathrm{H}_*(G),$$

where G is Kontsevic's graph complex.

For example, one can show that cohomology groups like $\mathrm{H}^{15}(\mathcal{M}_6, \mathbb{Q}) \neq 0$.

Now let's turn to abelian varieties. Here is a taster.

Theorem 65. One can compute $W_0\mathrm{H}_c^*(\mathcal{A}_g, \mathbb{Q})$ in many cases.

For this, one should compactify $\mathcal{A}_g$, which can be done explicitly via some combinatorial data to produce some toroidal compactification. Then one can write down some chain complex to execute the above computation.

We now turn to locally symmetric spaces $\Gamma\backslash D$ where D is a Hermitian symmetric domain and Γ is a discrete arithmetic subgroup; note that this quotient is a variety. For example, this includes the moduli of principally polarized abelian varieties (such as elliptic curves). One also is able to produce some level structure in the usual way. It is known how to compute a smooth toroidal compactification $\overline{\Gamma\backslash D}^{\Sigma}$ which depends on some combinatorial data Σ.

Definition 66. The boundary of the aforementioned compactification is the tropicalization $(\Gamma\backslash D)^{\mathrm{trop}}$.

So we are interested in studying some compactifications. This is a rather complicated procedure, but at the end, one can use it to compute cohomology.

2.7 Prym Representaions and Twisted Cohomology

This talk was given by Xiyan Zhong. Let Σ_g^b be a genus-g surface with b boundary components, and let Mod_g^b denote the space of homeomorphisms of Σ_g^b fixing the boundary, up to isotopy. We would like to study the action of this mapping class group and its effect on cohomology.

Suppose that we have some covering $\Sigma_{g'}^{b'} \to \Sigma_g^b$ with abelian Galois group. For a fixed ℓ, there is an action by $\mathrm{H}_1(\Sigma_g^b, \mathbb{Z}/\ell\mathbb{Z})$, so we may define some $\mathrm{Mod}_g^b(\ell)$ as the kernel of this action. We call this representation the "Prym representation." As a taste, we could be interested in the cohomology of Mod_g^b. One tool is a sequence

$$\mathrm{Mod}_g^b \to \mathrm{Mod}_{g+1}^b \to \cdots$$

given by simply adding on a hole repeatedly. Then we note that there is a known homological stability result for $\mathrm{H}^*(\mathrm{Mod}_g^b, \mathbb{Z})$ in the large g limit. It turns out that one can even work with $\mathrm{Mod}_g^b(\ell)$.

Theorem 67 (Putnam)**.** For large ℓ, the map

$$\mathrm{H}^*(\mathrm{Mod}_g^b, \mathbb{Z}) \to \mathrm{H}^*(\mathrm{Mod}_g^b(\ell), \mathbb{Z})$$

for large g.

Now, we may be interested in some cohomology like $\mathrm{H}^1(\Sigma_g^b, \mathbb{Q})$, but we would like to add some group action and in particular the Prym representation. For example, one has the following.

Theorem 68 (Putnam)**.** There is a stability result for

$$\mathrm{H}^*\left(\mathrm{Mod}_g^b, \mathrm{H}^1(\Sigma_g^b, \mathbb{Q})^{\otimes r}\right) \to \mathrm{H}^*\left(\mathrm{Mod}_g^b(\ell), \mathrm{H}^1(\Sigma_{g'}^{b'}, \mathbb{Q})^{\otimes r}\right).$$

Looking at our known results, we are able to state our own computation.

Theorem 69. For $r \geq 1$ and $g \gg k$, we compute $\mathrm{H}^k\left(\mathrm{Mod}_g^b(\ell), \mathrm{H}^1(\Sigma_{g'}^{b'}, \mathbb{Q})^{\otimes r}\right)$.

In particular, there is some stability, but it is not naively from the cohomology of Mod_g^b.

Example 70. If $k + r$ is odd, then

$$\mathrm{H}^k\left(\mathrm{Mod}_g^b(\ell), \mathrm{H}^1(\Sigma_{g'}^{b'}, \mathbb{Q})^{\otimes r}\right) = 0.$$

3 Hypergeometric Functions

These talks occurred on Thursday the 9th of January.

3.1 Factorial Affine Varieties with a Torus Action

This talk was given by Takanori Nagamine. This talk is not hypergeometric, but I wandered in. We are interested in classifying unique factorization domains. For example, here is a question known as the Zariski cancellation problem: if A is a k-algebra such that $A[x_1, \ldots, x_n]$ is isomorphic to a polynomial ring over k, then is A isomorphic to a polynomial ring over k? Here are some partial answers.

- If $\dim A \le 2$, the answer is yes.
- If $\dim A \ge 3$ and $\operatorname{char} k > 0$, then the answer is no, and there are counterexamples known due to Zariski.
- Lastly, if $\dim A \ge 3$ and $\operatorname{char} k = 0$, then the problem is open.

Let's generalize the problem to give us some flexibility.

Definition 71 (retract)**.** An A-algebra B is a *retraction* if and only if there is a projection $\pi\colon B \to A$ such that $\pi|_A = \operatorname{id}_A$.

Example 72. Polynomial rings are retractions of their coefficient ring.

So one can ask if being a retraction of a polynomial ring forces one to be a polynomial ring, exactly as before. This is known as the retraction problem. Of course, even less is known now.

For now, we work over an algebraically closed field k. We assume that A is a rational unique factorization domain (rational means $K(A)$ is isomorphic to a polynomial ring over k) of dimension $d \ge 2$. We will also assume that there is a $\mathbb{Z}^{d-1}$-grading which is "effective and unmixed" with $A_0 = k$. Note that these domains were classified already in some cases, such as $\dim A \le 3$ or $\dim A \ge 2$ in characteristic 0. Here is our main result.

Theorem 73. Fix a k-domain A of dimension $d \ge 2$.

(i) A is a rational unique factorization domain with a $\mathbb{Z}^{d-1}$-grading which is effective and unmixed with $A_0 = k$.

(ii) A is a rational unique factorization domain with $A^\times = k^\times$ with a $\mathbb{Z}^{d-1}$-gradig which is effective with $A_0 = k$.

(iii) A is isomorphic to a polynomial ring over $k[\Delta]$ for some "trinomial datum" Δ.

There remains a lot to exaplin.

Definition 74 (effective, unmixed)**.** Fix a $\mathbb{Z}^n$-graded ring A. Define M as the set of $g \in \mathbb{Z}^n$ such that $A_g \ne 0$.

(a) Then the grading is *effective* if and only if M generates $\mathbb{Z}^n$ as a group.

(b) Then the grading is *unmixed* if and only if $g + h = 0$ for $g, h \in M$ implies $g = h = 0$.

For example, effective means that we are using the "full" rank of $\mathbb{Z}^n$, and unmixed codifies some kind of cone condition. It remains to explain what a trinomial datum is.

Definition 75. A trinomial datum Δ consists of the following.

- An ordered partition $n = n_0 + \cdots + n_r$. Then we label some variables $\{T_{i1}, \ldots, T_{in_i}\}$ for each i.
- We choose vectors $(\beta_{i1}, \ldots, \beta_{in_i})$ in $\mathbb{Z}_{>0}^{n_i}$ for each i. Say d_i is the greatest common divisor of these variables, and then we assume that the $d_\bullet$s are pairwise coprime. We will write $T_i^{\beta_i}$ for the induced monomial.
- We choose distinct scalars $\lambda_2, \ldots, \lambda_r \in k^\times$.

Then we define $k[\Delta]$ as k adjoin the $T_\bullet$s modded out by the polynomials $T_0^{\beta_0} + \lambda_i T_1^{\beta_1} + T_i^{\beta_i}$ for each i.

One can check that this is a rational unique factorization domain of dimension $n - r + 1$. We have now stated all the adjectives for the main theorem. As a quick application, we note that $k[\Delta]$ is smooth if and only if $k[\Delta]$ is a polynomial ring over k. Additionally, under our grading assumptions, we solve the Zariski cancellation problem and retraction problem.

Let's outline the proof that (i) implies (iii) in the main theorem. We may as well assume that A is not already a polynomial ring over k. It is well-known that A is finitely generated over k. We now have the following steps.

1. We claim that there are homogeneous and pairwise coprime elements $x_1, \ldots, x_{d+\ell} \in A$ generating A as a k-lagebra. This uses the assumption $\overline{k} = k$, A is a unique factorization domain, A is unmixed, and $A_0 = k$.
2. Consider the fraction subring $K_0 \subseteq K(A)$ consisting of elements of the form a/b where $a, b \in A_g$ for some g. Then we claim that K_0
3. Combining the previous two claims, one finds monomials $M_0, \ldots, M_r$ in the $x_\bullet$s generating certain fraction subrings of $K(A)$. One can use these to complete the proof after a change of variables.

3.2 Hypergeometric Distributions and Joint Families of Elliptic Curves

This talk as given by Hasan Saad, and it was good but quick. Recall the classical Sato–Tate predicts the distribution of $\#E(\mathbb{F}_p)$ as p varies over primes. We are interested in "vertical" distributions which fix the finite field $\mathbb{F}_q$ and lets the variety vary. We will work with hypergeometric varieties.

Definition 76. Fix a prime p, and let ω generated $\mathbb{F}_p^\times$. Let α and β be collections of rational numbers with $\beta_1 = 1$. If $p \equiv 1 \pmod{M}$ where $M = \gcd(a, b)$, we may define the hypergeometric series as usual.

Then one can construct some elliptic curves which read off the hypergeometric functions in their point-counts. For example, this was used to compute some "vertical" distributions by doing statistics on families of elliptic curves.

One can go beyond elliptic curves. For example, the K3 surface

$$X_\lambda \colon s^2 = xy(x+1)(y+1)(x+\lambda y)$$

again reads off some hypergeometric data, so one can prove a distribution using similar techniques as before.

Let's recall the method. Let U_m be the Chebychev polynomial of the second kind and degree m. The idea is to express

$$\frac{1}{p} \sum_{\lambda \in \mathbb{F}_p} U_m \left(\frac{a_{X,\lambda}(p)}{2\sqrt{p}} \right)$$

in terms of the Fourier coefficients of some cusp forms. Then one can bound the sum using Deligne's bound on Fourier coefficients allows one to compute moments and determine the distribution.

Thus, here are some motivating questions.

- The above methods work with hyperogemetric data of length less than 4. What if it is longer?
- Catalan numbers seem to appear in the moments. Is there a reason?
- Where do these Chebychev polynomials come from?

We will answer these questions. For example, some main results are able to find limiting moments of certain hypergeometric functions over finite fields (but now with hypergeometric data of length four), and some Catalan numbers appear. One can then use this to compute some joint distributions, and one finds that they are independent in the large p limit.

Let's turn to methods. We will use the theory of étale sheaves to explain the presence of the Catalan numbers and Chebychev polynomials. Roughly speaking, and étale sheaf is a representation of the étale fundamental group. For example, one can realize a family of elliptic curves as an elliptic scheme $\mathcal{E} \to \mathbb{A}^1$. Then the Tate module $V_\ell\mathcal{E}$ is some ℓ-adic local system; for example, we find that

$$\operatorname{tr}(\operatorname{Frob}_q|V_\ell\mathcal{E}_\lambda)^r = \operatorname{tr}(\operatorname{Frob}_q|V_\ell\mathcal{E}_\lambda^{\otimes r})$$

for any $m \geq 0$. Now, one can compute these traces using the Grothendieck–Lefschetz formula. It turns out that the zeroth and second cohomology groups vanish, and the Riemann hypothesis explains the eigenvalues of the Frobenius on cohomology groups.

In order to work with two familes $\mathcal{E}_1$ and $\mathcal{E}_2$, the correct sheaves to look at are tensor powers. Now, we will want to take an irreducible decomposition of our tensor products (over the group $\mathrm{SU}(2)$), so we remark that

$$\operatorname{tr}(\operatorname{Sym}^m \operatorname{Std}(g)) = U_m\left(\frac{\operatorname{tr}\rho(g)}{2}\right),$$

which explains the presence of our Chebychev polynomials! Namely, one now uses some representation theory of $\mathrm{SU}(2)$ to decompose the sheaves $V_\ell\mathcal{E}_1^{\otimes m_1} \otimes V_\ell\mathcal{E}_2^{\otimes m_2}$ into irreducible representations of $\mathrm{SU}(2) \times \mathrm{SU}(2)$, plug into the above formulae, and then prove our results.

3.3 On the Parity of Coefficients of Eta Powers

This talk was given by Anna Medvedovsky. Fix a q-series $f(q) = \sum_n a_n q^n$ which is supported on the arithmetic progression $b \pmod m$. Powers of $\eta(q) := q^{1/24}\prod_k (1-q^k)$ are known to have this property when plugging in stuff like $\eta\left(q^{24/\gcd(24,r)}\right)^r$.

We now define an operator U_ℓ on power series given by

$$\sum_n a_n q^n \mapsto \sum_n a_{\ell n} q^n.$$

In particular, if f is supported on $b \pmod m$, then $U_\ell f$ has leading term $a_N q^{N/\ell}$ for some $N = N(f,m,\ell)$. For fixed prime p, we are interested in the density $D_p(f,m)$ of the set $S_p(f,m)$ of primes ℓ such that $a_{N(f,m,\ell)} \not\equiv 0 \pmod p$. Here is a main result.

Theorem 77. If f is a modular form, then the density $D_p(f,m)$ is a rational number.

One can show this by showing that $S_p(f,m)$ arises from the Chebotarev desnity theorem.

Let's take a moment to specialize to $p = 2$ and f a power of η in the form $\eta\left(q^{24/\gcd(24,r)}\right)^r$; then one wants to show that the function $D(r)$ sending r to this density is a function to rationals with denominator a power of 2. It looks likethis density $D(r)$ concentrates around certain powers, though we can only provide heuristics at the moment. Here are some partial results.

Theorem 78. One has $D(r) = 0$ if and only if r is a divisor or multiple of 32 or 48.

Theorem 79. One has $D(r) < 1$ and $D(2r) < 1/2$ and $D(4r) \leq 1/4$ for all r.

Further, one can even compute some special nonzero cases of D using Galois-theoretic methods. Let's outline our method.

1. To begin, we express $\eta\left(q^{24/\gcd(24,r)}\right)^r$ in terms of mod-2 modular forms of level 1 and 9. For this, one defines some explicit modular forms and does a computation.

2. Then one can reinterpret our density in terms of some Galois-theoretic densities $\delta(T_u f)$, where T_u is a Hecke operator. More precisely, $\delta(f)$ is the density of primes $\ell \in S_f$ such that $a_\ell \not\equiv 0 \pmod{p}$. However, $\delta(f)$ is not $D_p(f,m)$ verbatim because of some modular problems.

3. Then Galois methods are able to compute $\delta(f)$s. In particular, it turns out that $\ell \in S_f$ if and only if Frob_ℓ belongs to a particular conjugacy class in $\operatorname{Gal}(E_f/\mathbb{Q})$ for some field E_f given by f.

3.4 Explicit Images for the Shimura Correspondence

This talk was given by Swati. It was pretty notationally cumbersome, so I did not take many notes.

The Shimura correspondnence consists of some maps between modular forms. Namely, one maps $\operatorname{Sh}_t \colon S_{\lambda+1/2}(\Gamma_0(N), \psi\nu_\theta^{2\lambda+1}) \to S_{2\lambda}(\Gamma_0(N/2), \psi^2)$ satisfying

$$\operatorname{Sh}_t \circ T_{p^2} = T_p \circ \operatorname{Sh}_t.$$

These maps play a key role in the theory of half-weight modular forms. To motivate our work, let η be as usual. Given $f \in M_s(\Gamma_0(1))$ and $r \in \{1,2,\ldots,23\}$ with $\gcd(3,6) = 1$, then se $\lambda = \frac{r-1}{2}$. One can then consider modular forms of the form $\eta(24z)^r f(24z)$ and do a computation. In particular, one can show that their images under the Shimura correspondence have much lower level than is expected a priori. This result is due to Yang, and it essentially consists of long technical computations of traces of Hecke operators.

Our goal is to explicate the Shimura correspondence to optimize the proof of Yang. As before, $r \in \{1,2,\ldots,23\}$ and $\gcd(r,6) = 1$ and $s \geq 0$ is even, so we set $k = (r-1)/2 + s$. Note $M_k(\Gamma_0(r), (\cdot/r))$ has a basis $\{g_1,\ldots,g_d\}$ of normalized Hecke eigenforms, which one can write down explicitly. Then we define $G_i(z) \coloneqq g_i(z)g_i(6z) - g_i(2z)g_i(3z)$, and it turns out that one can compute $\mathcal{S}_r(\eta^r f)$ as a linear combination of the G_is, where $\mathcal{S}_r$ is a twisted version of the Shimura correspondence. One can recover a result for r divisible by 3 as well.

3.5 A Modular Framework of Functions of Knopp

This talk was given by Andreas Mono. It was also notationally cumbersome.

Let $\mathcal{Q}_D$ be the set of integral binary quadratic forms $[a,b,c](x) \coloneqq ax^2 + bxy + cy^2$ of discriminant $D = b^2 - 4ac$. Then $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{Q}_D$ by a linear substitution. Evaluation at some $(\tau, 1)$ satisfies

$$\left(Q\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)(\tau,1) = (c\tau+d)^2 Q(\tau,1).$$

For example, one can write down averages

$$f_{k,D}(z) \coloneqq \sum_{Q \in \mathcal{Q}_D} \frac{1}{Q(\tau,1)^k}$$

to produce something like an Eisenstein series. If $D > 0$, we have a cusp form of weight $2k$; and if $D < 0$, we have a meromorphic modular forms of weight $2k$ with poles which are CM points of discriminant D.

For $D > 0$, there is a kernel

$$\Omega_{k,D}(\tau,z) \coloneqq \sum_{D>0} D^{k-1/2} f_{k,D}(z) q^D$$

which produces Shimura and Shintani lifts between $S_{2k}(1)$ and $S^+_{k+1/2}(4)$. There are some other properties of interest.

Next, we define the Bol operator $\mathbb{D}^{k-1}$ as $\left(\frac{1}{2\pi i}\frac{d}{d\tau}\right)^{k-1}$. Then there is some identity

$$\mathbb{D}^{k-1}\left(\log\left(\frac{\tau-\alpha_Q^-}{\tau-\alpha_Q^+}\right)Q(\tau,1)^{k-1}\right)\approx\frac{1}{Q(\tau,1)^k}.$$

Here $\alpha_Q^\pm$ are the complex roots. By changing the sign of k, one can still average to produce some kind of Eisenstein series named $\psi_{k+1,D}$, but it is not quite modular, but the error of being modular is more or less controlled: there is an infinite series and a period function.

Let's try to fix this. Name $\omega_{k+1,D}(\tau,w)$ to be $\psi_{k+1,D}(\tau)$ minus some input from the infinite series. Then one can try to prove modularity in some formal way. One uses Parson's functions to ensure holomorphy of this function now defined on $\mathbb{H}\times\mathbb{H}$. This produces the required function $\Omega_{k+1,D}(\tau,w)$.

3.6 Special Values of Hecke L-series for Shinha Modules

This talk was given by Matt Papanikolas. By way of motivation, note that the elliptic curve $E\colon y^2=x^3-x$ over $\mathbb{Q}$ has complex multiplication by $\mathbb{Z}[i]$ defined over $\mathbb{Q}(i)$. Thus, its L-function comes from a Hecke character ψ_E of $\mathbb{Q}(i)$. We are interested in special values, so we note that it turns out

$$L(E,1)=\frac{1}{\sqrt{2}}\cdot\frac{\Gamma(1/4)^2}{\sqrt{\pi}}$$

by the Chowla–Selberg fomrula. We remark that there is a similar computation that one can do for Jacobians of Fermat curves, allowing one to write the L-function in terms of L-functions of Hecke characters ψ by hand. It was proven in the 1980s that $L(\psi,1)$ should be a $K^\times$ times some Gammas of the form $\Gamma(a/d)$.

We are interested in a finite-field analogue, so we translate everything over to $A=\mathbb{F}_q[\theta]$ in the natural way. For example, we recall that $|f|_\infty=q^{\deg f}$. Our cyclotomic fields now come from Carlitz modules, so let's review this notion.

Definition 80 (Carlitz module)**.** Let τ on $\mathbb{C}_\infty$ (which is the completion of the algebraic closure of $\mathbb{F}_q((1/\theta))$) be the qth power Frobenius. Then there is a map $C\colon A\to\mathbb{C}_\infty[\tau]$ by $C_\theta=\theta+\tau$. Then C makes $\mathbb{C}_\infty$ into an A-module different from the usual scalar multiplication, wchih we call a Carlitz module.

Given a Carlitz module C, we define $\exp_C(X)$ as some explicitly defined power series, which produces a map $\mathbb{C}_\infty\to\mathbb{C}_\infty$. Then one has a diagram of short exact sequences as follows.

$$\begin{tikzcd}
0 \arrow[r] & A\pi \arrow[r] \arrow[d] & \mathbb{C}_\infty \arrow[r] \arrow[d, "a"] & C(\mathbb{C}_\infty) \arrow[r] \arrow[d, "C_a"] & 0 \\
0 \arrow[r] & A\pi \arrow[r] & \mathbb{C}_\infty \arrow[r] & \mathbb{C}(C_\infty) \arrow[r] & 0
\end{tikzcd}$$

Here, π is a Carlitz period with some explicit expression as an infinite product of θs. One now finds our Carlitz extensiosn K_f of $\mathbb{F}_q[x]$ by adjoining the torsion of some $f\in\mathbb{F}_q[x]$; this turns out to be $\exp(a\pi/f)$ where $a\in A$ and $\deg a<\deg f$. For example, one can find an isomorphism $\rho_\bullet\colon(A/f)^\times\to\operatorname{Gal}(K/k)$, and it turns out that this is compatible with the Artin symbol.

As with Fermat curves, one is now able to find some "Carlitz cyclotomic" curves by looking for a curve over $\mathbb{F}_q$ with function field K_f. As one expects, one finds $\deg f$ points at infinity after completing the smooth plane curve. For example, there are some nice points

$$\xi_a:=(\theta,\rho_a(\zeta)),$$

where $\zeta:=\exp(\pi/f)$ is essentially a primitive "fth" root of unity.

For brevity, define $\mathcal{A}$ as the set $a\in A$ with $\deg a<\deg f$ and $(a,f)=1$ and $\mathcal{A}_+$ as the monic subset. Then Sinha constructed some rational function g with a well-behaved divisor. For example, this function can be written down explicitly as a linear combination of some exponentials and Carlitz action.

To continue, we note that there is a Gamma function

$$\Pi(x) = \prod_{n \in A_+} \left(1 + \frac{x}{n}\right)^{-1}$$

on $\mathbb{C}_\infty$. There are good reasons to use this as a function field analogue. For example, it has some interpolation formula. With this, Sinha constructs some modules which look like they should be something like an abelian variety with complex multiplication by K_f. (Namely, they are essentially quotients by a lattice where the lattice has multiplication by K_f.) One can also build Hecke characters ψ in our suitably cyclotomic way, and we find that there is a Hecke L-series which even makes sense in $\mathbb{C}_\infty$. Then the main result of the current talk is that $L(s, \psi)$ once again can be expanded out as a product of Πs.

3.7 Modular Forms, Hypergeometric Motives, and Rigid Surfaces

This talk was given by John Voight, and it was very good. Recall that elliptic curves over $\mathbb{Q}$ are modular, allowing us to produce a modular form $f \in S_2(\Gamma_0(N), \mathbb{Q})$ bijectively from an elliptic curve E over $\mathbb{Q}$ of conductor N; notably, the L-functions and Galois representations align. This talk will be about explicit modularity.

We quickly recall the definition of $L(E, s)$ as

$$L(E, s) = \frac{1}{L_p\left(E, p^{-s}\right)},$$

where $L_p(E, T) = 1 - a_pT + pT^2$ for p of good reduction. Let α_p and β_p be the roots. For ordinary p, it turns out that $v_p(\alpha_p) = 0$ and $v_p(\beta_p) = 1$, so we get a Hodge vector like $(1, 1)$. In general, if $f \in S_k(\Gamma_0(N), \chi, M)$ where the coefficients are in M, then we get a Hodge vector like $(g, 0, \ldots, 0, g)$ where the length of the vector is k.

Example 81. In the case $k = 2$ over $\mathbb{Q}$, we find that modular forms correspond to abelian varieties over $\mathbb{Q}$ of GL_2-type.

Example 82 (Schütt)**.** Now in the case $k = 3$ and $g = 1$ and $M = \mathbb{Q}$, we hope to find f from the Hodge vector $(1, 0, 1)$ in a surface X. It turns out that f is automatically CM, and χ is quadartic. Assuming the Riemann hypothesis for odd real Dirichlet characters, then there are exactly 65 such newforms f, coming from 65 imaginary quadratic fields with class group.

We are interested in finding the surface X in the second example. Then $H^2(X, \mathbb{Q})$ has $\mathrm{NS}(X)_\mathbb{Q} \subseteq H^{1,1}$, consisting of divisors modulo equivalence. What is left we put in a transcendental subspace $T(X)_\mathbb{Q}$. This permits the following definition.

Definition 83 (rigid)**.** A surface X is *rigid* if and only if $\mathrm{NS}(X)_\mathbb{Q}$ spans $H^{1,1}$.

Theorem 84 (Elkies–Schütt)**.** Associated to $f \in S_3(\Gamma_0(N), \chi, \mathbb{Q})$ is a rigid K3 surface X with the correct L-function.

Example 85. For example, the Fermat quartic surface comes from $\eta(4z)^6$.

Let's move on to $g = 2$ and $k = 3$ so that $(2, 0, 2)$.

Definition 86 (geometric genus)**.** Given a surface X, the *geometric genus* is $\rho_g = \dim_\mathbb{C} H^{0,2}$.

We are now looking for our rigid surface X over $\mathbb{Q}$ with geometric genus 2 coming from f. We conjecture that this should be true for only finitely many f up to twist. On one hand, it's hard to do so; on the other hand, there are some moduli arguments that suggest there should be few. Let's give some examples.

Example 87 (Kuga–Sato)**.** Consider $f \in S_3(\Gamma_0(9), \chi)$. Consider the universal elliptic curve $\mathcal{E}_1(9) \to Y_1(9)$, which does provide a reasonable candidate surface. However, we would still like to check if they are rigid, which is done using the Shioda–Tate formula.

Example 88 (elliptic surfaces)**.** Maybe we can go look for other elliptic surfaces and their twists. For example, maybe we start with $y^2 = x(x-1)(x-t)$, plug in $t = \left(s^2-1\right)^2$. It turns out to go to a desired modular form.

Example 89 (double covers)**.** One can try to build a double cover of $\mathbb{P}(1,1,2)$. Then one can blow-up to get to smoothness, do a long construction, and eventually we get a good surface.

Example 90 (hypergeometric motives)**.** There are 32 hyperogemetric familes over $\mathbb{Q}$ with Hodge vector $(2,1,2)$. One can try to degenerate these families, but they do not seem to come from modular forms. Roughly speaking, one can look at the endoomorphism algebras we get from a Hodge structure looking like $(2,0,2)$, but this is quite rare.

3.8 Hypergeometric Differential Equatinos and Invertible K3 Surface Pencils

This talk was given by Ursula Whitcher. We are thinking about a dimensional tower, where one goes from elliptic curves to K3 surfaces to Calabi–Yau threefolds. (For example, elliptic curves are cubics in $\mathbb{P}^2$, K3 surfaces are quartics in $\mathbb{P}^3$, and so on.)

Let's begin with elliptic curves. Then the elliptic curves has some periods, and one can study them in families via the Picard–Fuchs differential equation. For a K3 surface, one has essentially inflated the Hodge diamond to dimension 2 with the condition $\dim H^{11} = 20$. Once again, a family of K3 surfaces gives rise to a hyperplane class in $H^{11}(X)$, and there is still a period by taking an integral from which one gains a Picard–Fuchs differential equation. Our end goal is to produce explicit formulas for K3 surfaces L-functions, but for now we will focus on some geometric things.

To set ourselves up, note that a matrix $A = [a_{ij}]_{0 \le i,j \le n}$ with nonnegative integer matrices produces a polynomial

$$F_A(x) \coloneqq \sum_{i=0}^{n} \prod_{j=0}^{n} x_j^{a_{ij}}.$$

For example, the diagonal case produces the Fermat hypersurfaces. For some language, we say that F_A is invertible if and only if A is invertible and there are some other nice geometric properties (namely, there are weights q_j such that $\sum_{j=0}^{n} q_j a_{ij}$ is constant in i, and there is only one critical point of F_A which is at the origin). Under these hypotheses, the weights are able to define a quasismooth hypersurface X_A in the appropriately weighted projective space.

Example 91. Delsarte studied polynomials with weights $(1,\ldots,1)$.

Example 92. If F_A is invertible, then $F_{A^\intercal}$ is too. It is able to define some mirror symmetry data of X_A.

Remark 93. The connection to mirror symmetry interested some physicists, and they classified them as being sums of certain given classes. There are ten which produce K3 surfaces; for example, there is the Fermat quartic but also a few stranger ones.

Deforming our equation by something like $-d^\intercal \psi x$ (where d is the weights and ψ is the parameter), we can produce a pencil. It is known due to Gährs that a Delsarte invertible pencil of K3 surfaces (or Calabi–Yau varieties) have periods coming from a hypergeometric Picard–Fuchs equation (with explicit hypergeometric parameters). One can work these out coming from the above remark. Here is our first main theorem, which looks at periods beyond the hyperplane class in H^{11}.

Theorem 94. For each of the pencils living in $\mathbb{P}(1,1,1,1)$, the primitive middle-dimensional cohomolgoy has 21 periods which satisfy a hypergeometric Picard–Fuchs differential equation.

As before, one can explicitly compute the hypergeometric differential equations. Here are two methods.

- The diagram method: organize the periods by their derivatives as living in the finite-dimensional vector space, and we must eventually find a relation with some linear algebra. This does not really tell us why the differential equations exist.
- One can identify some hypergeometic operators on the cohomology group of an invertible pencil. Note not all these operators are not immediately geometric!

3.9 Inversion Formulas for the Modular j-Function

This talk was given by Alejandro de las Peñas Castaño. We recall that the there is a modular j-function $\mathbb{H} \to \mathbb{C}$ with symmetry group $\mathrm{SL}_2(\mathbb{Z})$. It has special values $j(i) = 1728$ and $j(\rho) = 0$ (here, $\rho = \zeta_3$). For motivation, we recall that j parameterizes elliptic curves and generate abelian extensions of imaginary quadratic fields; there are also connections to monstrous moonshine.

Recall that j is a bijection $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^* \to \mathbb{C} \cup \infty$. We may want to compute the inverse of this map. For example, it is conjectured that one can compute the Taylor series $T(t)$ of j around $\tau \in \{i, \rho, \infty\}$, and one can find special functions $\omega(t)$ such that $T(\omega(t))$ is rational in t. Let's be more precise. Let s_{τ_*} be the conformal maps $\mathbb{H} \to \mathbb{D}$ sending τ to 0, normalized by some Chowla–Selberg periods. Then they conjecture that

$$j\left(s_i^{-1}\left(\frac{h_i(t)}{g_i(t)}\right)\right) = 64\frac{(3+4t)^3}{(1-4t^2)^2},$$

and there is a similar conjecture for ρ; here h_i and g_i are some explicit power series. This was shown recently, where the key idea was that the right-hand polynomial arises from certain families of elliptic curves.

Quickly, recall the hypergeometric series

$${}_2F_1(a,b,c;z) = \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n}\frac{z^n}{n!},$$

where $(a)_n$ is the Pochhammer symbol; it satisfies some differential equation. These hypergeometric functions are able to produce inversion formulas for j, thereby proving the conjecture of the previous paragraph.

The main result of this talk is a similar result extending the above inversion formulae. For example, they prove the following.

Theorem 95. One has

$$j\left(\frac{s_i^{-1}(C_i(t))+1}{2}\right) = 64\frac{(16t^2-3)^3}{4t^2-1},$$

where C_i is some explicit quotient of hypergeometric functions. There is a similar result for ρ.

The moral of the story is that inverting $j(\tau) = \alpha$ basically comes down to solving a quadratic or cubic and then plugging into C_i. For example, one solve $j(\alpha) = 8000$ to find $\alpha = \sqrt{-2}$. Let's list the main inputs.

- There is a hypergeometric identity for ${}_2F_1(a,b,c;z)$ in terms of ${}_2F_1(a,b,c;1/z)$ and ${}_2F_1(a,b,c;1-1/z)$.
- They also used an existing inversion formula.

3.10 The Explicit Hypergeometric Modularity Method

This talk was given by Brian Grove. Let's begin by taking about hypgergeometric motives. Roughly speaking, one expects that a hypergeometric datum $(\alpha_\bullet, \beta_\bullet)$ should give rise to periods and so on over $\mathbb{C}$, point-counting over finite fields, and there are also p-adic incarnations. We are interested in finite-field modularity results, which should relate our hypergeometric functions to modular forms.

Let's work with the elliptic curve $y^2 = x(1-x)(1-\lambda x)$, and one can count its points via a finite-field hypergeometric function essentially by writing out solutions for y^2 using character sums. Thus, we see that we can realize the trace of a Frobenius to the hypergeometric function, and we further expect to find a modular form keeping track of this.

More generally, Katz produced a family of ℓ-adic representations ρ_{HD} of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_M))$ where $M = \operatorname{gcd}(\alpha_\bullet, \beta_\bullet)$ arises from the datum. Then it turns out that the trace of Frobenius from this Galois representation essentially calculate the values of the hypergeometric function over finite fields. On the other hand, the elliptic curve or modular form also has a Galois representation ρ_f of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

We are interested in relating these two Galois representations. Here are a few methods.

Example 96. One could imagine going through modularity of (certain) varieties, such as by going through the family of K3 surfaces

$$X_\lambda \colon s^2 = xy(x+1)(y+1)(x+\lambda y).$$

Then one would need to check which λ actually have modular forms.

Example 97. There is also a way to use the Eichler–Selberg trace formula, which roughly uses a comparison between isomorphism classes of elliptic curves and Hurwitz class numbers.

Note that the above techniques place the modular form secondary, and it is found essentially by coincidence. We would like a way to predict the modular form directly from the hypergeometric datum.

Example 98. Consider the datum $((1/2, 1/2, /1, 8), (1, 1, 1))$ and $\lambda = 1$. There is a weight computed combinatorially; it can be found to be 3. Similarly, one can compute some levels. So we are looking for a modular form of weight 3 and level $N = 2^j$ and $j \leq 8$. One numerically finds that the modular form we are looking for is 64.3.d.a at least when $p \equiv 1 \pmod 8$.

Let's try to explicate the previous example. Here are the steps.

1. One can begin with the hypergeometric function ${}_2F_1$. There is a way to expand it out as an integral.
2. Then we hope to be able to evaluate our hypergeometric function at some special point using known values, relating it to modular forms.
3. We are now able to evaluate the integral, yielding the required modular form.

Having a method like this allows one to prove families of results finding the modular form from a hypergeometric datum. This is the main result.

Let's list some inputs for a more general result.

- We work p-adically. By some bounding of Deligne, it is enough to check $\pmod{p^2}$.
- In the finite-field setting, one uses the Gross–Koblitz formula and some p-adic anaysis, allowing one to evaluate $H_p \pmod{p^2}$.
- Then one proves a Dwork-type supercongruence.

3.11 The Arithmetic of Hypergeometric Galois Representations in Low Dimensions

This talk was given by Ling Long. We are interested in Galois representations attached to hypergeometric datum; they can be computed rather explicitly. One expects motivic L-functions to be automorphic, so let's try to do this for our examples. We will focus on cases for irreducible representations of GO_4.

As usual, choose (α, β) to be a hypergeometric datum and define $M = \gcd(\alpha, \beta)$ as usual. We will say that (α, β) is defined over $\mathbb{Q}$ if and only if the polynomials

$$\prod_j \left(T - e^{2\pi i \alpha_j}\right) \qquad \text{and} \qquad \prod_j \left(T - e^{2\pi i \beta_j}\right)$$

live in $\mathbb{Q}[T]$. We say that (α, β) is primitive if and only if $\alpha_i - \beta_j \notin \mathbb{Z}$ always; this roughly corresponds to the corresponding representation being irreducible. Note that there is a combinatorial way to write down some Hodge numbers of (α, β), and we recall that there is a finite-field analogue as

$$H_p(\alpha, \beta, \lambda; \omega) = \frac{1}{1-p} \sum_{k=0}^{p-2} \omega^k((-1)^n \lambda) \prod_{j=1}^{n} \frac{g(\omega^{(p-1)\alpha_j + k}) g(\overline{\omega}^{(p-1)\beta_j + k})}{g(\omega^{(p-1)\alpha_j}) g(\overline{\omega}^{(p-1)\beta_j})},$$

where $g(\cdot)$ is the Gauss sum. We note that if (α, β) is primitive, then this is rational and thus independent of ω. Let's now give the corresponding motive.

Theorem 99 (Katz, Beukers–Cohen–Mellit)**.** For a primitive datum (α, β) defined over $\mathbb{Q}$ and $\lambda \in \mathbb{Q}^\times$, there is a d-dimensional compatible family of ℓ-adic representations ρ_λ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that

$$\operatorname{tr} \rho_\lambda(\mathrm{Frob}_p) = H_p(\alpha, \beta; 1/\lambda).$$

Here, $d = n$ if $\lambda \neq 1$ and is $n-1$ if $\lambda = 1$.

The moral of the story is that these hypergeometric functions over finite fields are seen to be on the Galois side of the Langlands program. We would now like to know if they are automorphic.

We would like to work with GO_4, so we need some discussion of parity. As such, we note that Katz has a combinatorial way to determine if ρ_λ preserves a bilinear form. In particular, it usually preserves a symmetric bilinear form; it only preserves an alternating form under some explicit but rare conditions. We are now able to state a main result.

Theorem 100. One can classify ρs as follows.

(i) ρ is an induction from a character; then ρ is found to be automorphic.

(ii) ρ is not of "type 0" and $\det \rho$ is a power of a cyclotomic character; then ρ is found to be a tensor product of Hecke eigenforms of explicit weights.

(iii) ρ is not of "type 0" nor "type 1"; then there is a quadraic field F and a character $\chi\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}_\ell^\times$ such that

$$(\rho \otimes \chi)|_{G_F} \cong \rho_1 \otimes \rho_1^\tau,$$

where $\rho_1\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ is a Galois representation and τ is some Galois element. Now if F is real, then we find ρ is potentially automorphic.

Notably, we can work out these types explicitly. The talk also worked out some cases with a hypergeometric datum involving $\frac{1}{d}$s.

4 Rethinking Number Theory

This session happened on Friday the 10th of January.

4.1 Zeroes of L-Functions Attached to Maass Forms

This talk was given by Amita Malik. For motivation, we recall that $\zeta(s)$ admits a Dirichlet series, Euler product, meromorphic continuation with prescribed poles, and a functional equation of the form $\xi(s) = \xi(1-s)$ for a completed zeta function ξ of ζ.

> **Remark 101.** Guth and Maynard have recently made a breakthrough in estimating the number of zeroes in a line to the right of $\operatorname{Re} s = \gamma$.

We are interested in computing the number of zeroes in some box of the form $[0,1] \times [-T,T]$. By the functional equation, it's enough to consider a box of the form $[0,1] \times [0,T]$. Currently, we can estimate this number $N(T)$ as

$$N(T) = \frac{T}{2\pi} \log \frac{T}{4\pi e} + O(\log T).$$

Under the Riemann hypothesis, Littlewood showed an error term $O(\log T / \log\log T)$, but it is expectation is $O(\sqrt{\log T \log\log T})$.

For derivatives $\zeta^{(k)}(s)$, one can show a similar estimate

$$N(T) = \frac{T}{2\pi} \log \frac{T}{4\pi e} + O_k(\log T)$$

for the number of zeroes in the box. Letting E_k be this error term, it was recently shown that the Riemann hypothesis gives error term of $O_k(\log T / \log\log T)$.

> **Remark 102.** For motivation, we remark that zero-free regions for ζ' also imply the Riemann hypothesis.

There is a similar story for other L-functions, such as the Dirichlet L-function and the Selberg zeta function of a compact Riemann surface. Here is our main result.

> **Theorem 103 (Malik–Murty).** Let $L(s,f)$ be the L-function of a primitive Maass form f. Let $N_1(T,F)$ be the number of roots in $[0,1] \times [-T,T]$. Assuming the generalized Riemann hypothesis,
>
> $$N_1(T,f) = \frac{T}{\pi} \log \frac{T}{2\pi m e} + O\left(\frac{\log T}{\log\log T}\right).$$
>
> Here, m is the smallest m with nonzero Dirichlet series coefficient.

Quickly, we recall that f still admits a Dirichlet series $\sum_n \lambda_f(n)/n^s$, Euler product, and functional equation. We note that it is expected $\lambda_f(n) = O(n^\varepsilon)$, but one only knows $\lambda_f(n) = O\left(n^{7/64+\varepsilon}\right)$.

Let's sketch some inputs. Consider

$$G(s,f) := \frac{-m^s}{\lambda_f(m) \log m} L'(s,f),$$

with m as before. Then one uses the argument principle to see

$$N_1(T,f) = \frac{T}{\pi} \pm \frac{1}{\pi} \arg G\left(\frac{1}{2} + iT, f\right) \pm \frac{1}{\pi} \arg L\left(\frac{1}{2} + iT, f\right) + O(1).$$

One can already bound the argument for the L term (because one has a zero-counting result for L), so the name of the game is now to control the arguments of G. The idea is to pass to G/L. Eventually one needs to control gaps between zeroes of G, which we remark uses techniques of Yitang Zhang.

4.2 Automorphic Forms and String Scattering Amplitudes

This talk was given by Maryam Khaqm. Our motivation comes from string theory. Three of the four fundamental forces can be found in discrete quantum fields, but gravity does not fit into the current framework.

String theory is a suggestion on how to add gravity. For example, one can explain how particles (now strings) interact. The math works in $\mathbb{R}\times\mathbb{R}^{9-d}\times\mathcal{T}^d$, where d is some parameter. When one adds in some symmetries, one becomes interested in some moduli spaces

$$G_d(\mathbb{Z})\backslash G_d(\mathbb{R})/K$$

where G_d is some group and K is a maximal compact.

We are interested in computing some scattering amplitudes to automorphic forms that arise from this string theory construction. For example, one can find some Eisenstein series. One expects the arising automorphic forms to be constants, Eisenstein series, or products of Eisenstein series. In 2018, the motivating result worked all this out for $\operatorname{SL}_2(\mathbb{R})$. We would like to work out $\operatorname{SL}_3(\mathbb{R})$, now working in

$$\operatorname{SL}_3(\mathbb{Z})\backslash\operatorname{SL}_3(\mathbb{R})/\operatorname{SO}_3(\mathbb{R}).$$

The main result of the talk is a conjecture on what the sort of things we are looking for, which is again some constants, some discrete series, and some continuous "Eisenstein" series. In the $\operatorname{SL}_2(\mathbb{R})$ case, it is known how to do such a decomposition for operators coming from $L^2(\Gamma\backslash\mathbb{H})$, but products of Eisenstein series do not live there; the trick is to subtract out some easy pieces. However, this trick becomes infeasible in the $\operatorname{SL}_3(\mathbb{R})$ case.

5 Mathematics Informed by Computation

This session happened on Friday the 10th of January.

5.1 Models of Modular Curves

This talk was given by David Zywina. Given a subgroup $G\subseteq\operatorname{GL}_2(\mathbb{Z}/N\mathbb{Z})$, there is a modular curve X_G; we'll assume that $\det G=(\mathbb{Z}/N\mathbb{Z})^\times$ and $-1\in G$ for simplicity, which gives smoothness, projectivity, and integrality. It has a modular interpretation, roughly speaking by asking for the Galois representation of the N-torsion of an elliptic curve E to be contained in G.

Example 104. One may be interested in $X_0(N)$, which has G to be upper-triangular matrices. We note $X_0(N)(\mathbb{Q})$ has been classified by Mazur and Kenku.

Example 105. Given a non-split Cartan subgroup C for a prime ℓ, and we let G be its normalize. Then one may be interested in $X_{\text{ns}}(\ell)=X_G$, for example for Serre's uniformity problem.

There are many equivalent constructions of X_G, but we would like an explicit model. There is a large industry trying to find models of X_G. We give a method to compute it.

Let's outline the approach, which is analytic. For example, there is an analytic description of X_G by lifting G to a congruence subgroup $\Gamma_G\subseteq\operatorname{SL}_2(\mathbb{Z})$, and then $X_G(\mathbb{C})$ is $\Gamma_G\backslash\mathbb{H}^*$. We also note that there is a space of modular forms $M_k(\Gamma_G)$ for $k\geq 2$ with symmetry group Γ_G. In fancy language, we want global sections of $\Omega_{X_G}^{\otimes k/2}(D_k)$, where D_k is some specified divisor to control cusps; this is a good definition because it is defined over $\mathbb{Q}$. So here are our steps.

1. Note that "weight-1" Eisenstein series allow one to explicitly compute $\mathbb{Q}$-generators of $M_{k,G}$.
2. Keeping track of cusps will allow us to embed $X_G\hookrightarrow\mathbb{P}_{\mathbb{Q}}^{\dim V-1}$ for some subset V of modular forms.
3. Then one hopes to cut down the target space.

David Zywina then gave some examples. The equations are (usually) pretty nice. For example, one is able to prove the following.

Theorem 106. Up to conjugacy, there are exactly 524 congruence subgroups $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ with $-I \in \mathbb{Z}$ such that X_Γ is hyperelliptic.

The idea is that gonality bounds lets us bound the genus, reducing to a finite computation. We remark that the result for congruence subgroups of the form $\Gamma_0(N)$ has been known.

5.2 Weierstrass Points on Shimura Curves

This talk was given by Holly Paige Chaos. Given a curve, there is a notion of Weierstrass points. For example, let X be a Riemann surface of genus g. Given $P \in X$, we suppose that there is a function f on X with a simple pole at P and no other poles, then g defines a birational map to $\mathbb{P}^1$; similarly, if it is a double pole, then X is hyperelliptic. In general, one can ask for a nonzero rational function f on X with a pole of order nP and no other poles; in general, one does not expect this for $n \leq g$, though $n > g$ comes from some geometry.

Definition 107. A point $P \in X$ is a *Weierstrass point* if and only if there is some such positive $n \leq g$. We may write $\mathrm{wt}(P)$ to measure sthe sum of the n which do not exist.

Example 108. The set of Weierstrass points on a curve has $2g+2$ points if and only if the curve is hyperelliptic. In this case, they are the fixed points of the hyperelliptic points, and the gaps are $\{1, 3, \ldots, 2g-1\}$, so the weight is $\frac{1}{2}g(g-1)$.

It is now a natural question to ask what the Weierstrass points of the modular curves $X_0(N)$ are.

Theorem 109 (Atkin, Lehner, Newmann)**.** If N is sufficiently composite, then the cusps 0 and ∞ of $X_0(N)$ are Weierstrass.

Theorem 110 (Ogg)**.** If N is prime, then the Weierstras points are supersingular $\pmod p$ and do not include cusps.

We are going to look at the Shimura curve parameterizing (principally polarized) abelian surface A with quaternionic multiplication by an indefinite quaternion algebra of discriminant D; we may say that A has QM. For example, it turns out that A is supersingular if and only if A is superspecial, meaning that its field of moduli comes from $\mathbb{F}_{p^2}$, implying there are only finitely many. As usual, we will allow our moduli problem some level structure $\Gamma_0(N)$, allowing us to build a Shimura curve $X_0^D(N)$.

Let's now list some inputs for our computation.

- In many situtations, it turns out that Weierstrass points on our Shimura curve specialize to singular points on the reduction $X_0^D(N)_{\mathbb{F}_p}$.
- The $X_0^D(p)$s do not have cusps, so techniques from modular forms are a little harder to apply.
- We will work in a situation when $X_0^D(p)$ is hyperelliptic, and the hyperelliptic involution comes from an Atkin–Lehner involution.

Let's now summarize a computation. In characteristic 0, one finds $X_0^6(11)$ is a genus-3 hyperelliptic. Its Weierstrass points turn out to be QM abelian surfaces with CM by $\mathbb{Q}(\sqrt{-66})$; it turns out that such a thing must decompose into a product of elliptic curves. There are techniques to determine when two such products of CM elliptic curves are isomorphic. One can also reduce $\pmod{11}$ to find superspecial points.

5.3 Murmurations of Dirichlet Characters

This talk was given by Kyu-Hwan Lee. Let's begin by recalling murmurations of elliptic curves. Fix an elliptic curve E defined over $\mathbb{Q}$, with rank r, conductor N_E, and define $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$ as usual.

We will fix a prime p for a moment and let the conductor vary over a large interval $[N_1, N_2]$ where N_1 and N_2 have medium size. Then one averages $a_p(E)$ as E varies over particular ranks r, which we call $f_r(p)$. Then the values of $f_r(p)$s oscillate as p gets larger; $f_1(p)$s look inverted to $f_0(p)$, but the oscillating pattern of $f_0(p)$ and $f_2(p)$ look similar. We remark that the patterns disappear if elliptic curves are weighted by something other than conductor.

To account for root numbers, we let $e_w(p)$ denote the same average, but now we are only asking for $r \equiv w \pmod 2$ for $w \in \{0, 1\}$. It turns out that one gets the same oscillation pattern no matter where the interval $[N_1, N_2]$ is placed, and one can see similar murmurations for more general modular forms. One continues to see some oscillation for other weights, abelian surfaces, etc.

Remark 111. The story of elliptic curves remains open, but we remark on some of what is known. Well, Zubrilina has proven that weight-k newforms see murmurations for even k, using the trace formula. There are also explained murmurations for Mass forms.

Let's now move to Dirichlet characters. Let $\mathcal{D}_+(N)$ and $\mathcal{D}_-(N)$ be the set of primitive even and odd Dirichlet characters $\pmod N$, as before; let $\mathcal{Q}_\pm(N)$ be the corresponding subset of quadratic characters. Now one looks at averages

$$\sum_{N\in[X,2X)} \sum_{\chi\in\mathcal{Q}_\pm(N)} \frac{\chi(p)}{g(\chi)},$$

where $g(\chi)$ is the Gauss sum; here, $\chi(p)/g(\chi)$ is the Fourier coefficient of $\overline{\chi}$. One finds murmurations, but they are noisy. Let's try to fix this.

1. One can work with all complex characters in $\mathcal{D}_\pm(N)$ Working with dyadic intervals looks a bit bizarre, but one can make the oscillation easier by working in short intervals of the form $\left[X, X + X^\delta\right]$ for fixed $\delta > 0$. (One recovers dyadic intervals by integration.) Then the trace formula approach explains the murmurations.
2. Alternatively, one can use a smooth cutoff function Φ to smooth out the average. Then one again uses some trace formula approach.

5.4 The Least Prime in the Chebotarev Density Theorem

This talk was given by Robert J. Lemke Oliver. We begin by setting some notation. Fix a finite Galois extension $K/\mathbb{Q}$. For each unramified prime p, one gets a conjugacy class Frob_p. Then the Chebotarev desnsity theorem says that the fraction of primes p with specified conjugacy class is proportional to the size of the conjugacy class C.

We would like to upper-bound the size of the first prime p with Frob_p living in a specified conjugacy class. The existing approach on the error term requires zero-free regions of the Hecke L-functions. Here is a taster.

Theorem 112. There is a prime p with $\operatorname{Frob}_p \in C$ such that $p \ll \left|\operatorname{Disc} K\right|^{16}$.

Theorem 113. Suppose $A \subseteq \operatorname{Gal}(K/\mathbb{Q})$ is an abelian subgroup intersecting C nontrivially. Then there is p with $\operatorname{Frob}_p \in C$ such that $p \ll_{[K:\mathbb{Q}]} \left|\operatorname{Disc} K\right|^{1042/|A|}$.

Example 114. If $\operatorname{Gal}(K/\mathbb{Q}) \cong S_n$, then one can optimize A to get the bound down to $\left|\operatorname{Disc} K\right|^{1042/n}$.

We provide a new method to prove the following result.

Theorem 115. Suppose $\operatorname{Gal}(K/\mathbb{Q}) \cong S_n$. Then there is p with $\operatorname{Frob}_p \in C$ and $p \ll_n \left|\operatorname{Disc} K\right|^{1042/\exp(n/4)}$.

One can optimize a little more depending on the cycle type of C. For example, one can get all the way down to $|\mathrm{Disc}\,K|^{1/2+\varepsilon}$ in the worst case, and then case where C is the n-cycle gets factorial decay in the exponent!

We will not use an interesting zero-free region of L-functions. Let's give a taster.

Example 116. Let's bound the least prime P which is inert in $\mathbb{Q}(\sqrt{D})$. Well, suppose each $p \le X$ is split or ramified. Then $\chi_D(m) = 1$ for each $m \le X$, so the character sum

$$\sum_{m \le X} \chi_D(m) = \sum_{\substack{m \le X \\ \gcd(m,D)=1}} 1$$

is large. Now one can compare this with the Pólya–Vinogradov inequality to require $p \ll D^{1/2+\varepsilon}$. We remark that one can improve the inequality due to Burgess and Vinogradov.

Let's now generalize this approach. Suppose we can find multiplicative functions F_+ and F_- such that $F_+(p)$ and $F_-(p)$ only depending on the conjugacy class Frob_p, and they should only be unequal when $\mathrm{Frob}_p \in C$.

Further, we would like sums over $F_-(n)$ to be small and sums over $F_+(n)$ to be large. For example, it would be nice for $L(s, F_-)$ to be entire and for $L(s, F_+)$ to be entire except for some controlled poles (and notably one at $s = 1$). We do remark that one has the needed continuation is known in the one-dimensional case by some class field theory, so one gets continuation for monomial virtual characters, and then tools from Brauer's theorem let us go a little further.

For example, certain groups G will have all their irreducible characters be nonnegative linear combinations of monomial characters, but this is really a condition on F_+ and F_-. Then to ensure the poles, one would like $\langle F_-, 1\rangle_{S_n} = 0$ and $\langle F_+, 1\rangle = 0$. On the other hand, we would like to minimize the total degrees of F_+ and F_-. So for fixed n and C, this is some linear programming optimization problem! One can run this computation and see some patterns, for example when C is an n-cycle, allowing us to prove the theorem above.

6 Arithmetic Aspects of Enumerative Geometry

This talk was given by Kristen Wickelgren.

Enumerative geometry is interested in counting algebro-geometric objects satisfying certain conditions, such as solutions to polynomials, lines in planes, etc. However, we note that these solutions might be defined over large fields, such as $\overline{\mathbb{Q}}$. We would like to keep track of fields of definition, for which we will use $\mathbb{A}^1$ homotopy theory.

By way of example, we wokr with a scheme $X \subseteq \mathbb{P}^3$ cut out by a homogeneous degree-3 polynomial. We recall the following result.

Theorem 117. Over $\mathbb{C}$, any smooth cubic surface contains exactly 27 lines.

Remark 118. However, over $\mathbb{R}$,

Let's discuss this result a bit. Segre described a dual space taking lines $L \subseteq X$ to its tangent space, which we note will intersect X twice. Thus, this association becomes a double-cover of $\mathbb{P}^1$; letting ι be the induced involution, we note that over $\mathbb{R}$ produces either complex conjugates or both real. In the complex conjugate case, this is called "elliptic," and in the real case, it is "hyperbolic." (Physically, elliptic means that a tangent plane following the line has a "spin" as one follows it.) Here is a result.

Theorem 119. Over $\mathbb{R}$, the number of hyperbolic lines minus the number of elliptic lines equals 3.

For example, this shows that there are at least three (hyperbolic) lines.

Now for a general field k, let $k(L)$ be the field generated by the coefficients of the equations cutting out L. Then the fixed point of ι is yields a quadratic extension which we name $k(L)(\sqrt{a})$.

Definition 120. We call a the "type" of L.

Let's now shift gears to talk about $\mathbb{A}^1$-homotopy theory. Morel and Voevodsky defined some stable $\mathbb{A}^1$-homotopy theory $\mathrm{SH}(k)$ which includes both k-schemes and topological spaces. Here are some features.

- This allows gluings and crunchines of schees.
- There are reasonable open covers of smooth schemes.
- $\mathbb{A}^1$ is homotopic to a point.
- To stabilize, we stabilize so that $\wedge\mathbb{P}^1$ is invertible.

Roughly speaking, $\mathrm{SH}(k)$ is the stabilization of $\mathbb{A}^1$-invariant sheaves on smooth k-schemes.

Remark 121. Let's motivate this construction. For one, it is a natural place for many cohomology theories, such as Betti, ℓ-adic, K-theory, algebraic cobordism, motivic cohomology, and so on. More precisely, any theory satisfying the above points (which is expected from a cohomology theory) will factor through this homotopy theory; this also makes this a good home for motives.

Remark 122. As another motivation, we note that there is a "flagship" reslt of Voevodsky's proof of the Bloch–Kato conjectures.

Continuing, we note that there is a degree isomorphism $\deg$ from $[\mathbb{P}^n, \mathbb{P}^{n-1}, \mathbb{P}^n/\mathbb{P}^{n-1}]$ to $\mathrm{GW}(k)$, which is the group completion of non-degenerate symmetric bilinear forms over k; for example, $\langle 2\rangle + \langle 3\rangle = \langle \operatorname{diag}(2,3)\rangle$. So there is a dimension map from $\mathrm{GW}(k) \to \mathbb{Z}$. Here are two pieces of notation.

- For $k \subseteq \mathbb{R}$, one finds that there is also a sign map $\mathrm{GW}(k) \to \{\pm 1\}$ depending on the number of $(+1)$s or (-1)s.
- For a finite separable extension L/k, there is a trace map $\mathrm{T}_{L/k}\colon \mathrm{GW}(k) \to \mathrm{GW}(L)$ which just composes the bilinear form from $\mathrm{GW}(k)$ with the trace map.

We now turn to $\mathbb{A}^1$-enumerative geometry. Here is the sort of thing we can say.

Theorem 123. Let X be a smooth cubic surface over a field k not of characteristic 2. Then

$$\sum_{L \subseteq X} \mathrm{T}_{k[L]/k} \langle \mathrm{Type}(L)\rangle = 15\langle 1\rangle + 12\langle -1\rangle.$$

Morally, one should view this as providing weighted counts of lines. For example, one can take dimensions to recover 27 lines over the algebraic closure and take signs to get the difference of hyperbolic and real lines.

Let's say something about techniques. We take a moment to talk about Gromov–Witten invariants. Choose a projective variety X over $\mathbb{C}$, an integer n, and $\beta \in H_2(X)$. Then we may define $\overline{M}_{g,n}(X,\beta)$ as consisting of curves $u\colon C \hookrightarrow X$ with n marked points such that C is a genus-g nodal curve, u is stable, and $u_*[C] = \beta$. From here, we note that there are projection maps $e_i\colon \overline{M}_{g,n}(X,\beta) \to X$ by sending C with its marked points $\{p_1, \ldots, p_n\}$ to $u(p_i)$. There are a few other related such maps, and we note that these also lift to $\mathbb{A}^1$-homotopy theory. Then one uses these invariants to prove the result.

Let's list some other things one can prove, admittedly only on del Pezzo surfaces.

Example 124. There is $\langle 1\rangle$ conic through five points in the plane.

Example 125. For $A = (k, \ldots, k)$, one can compute the invariant $N_{0,X,\beta}(A)$ for $X = \mathbb{P}^2$, which roughly counts some number of some kind of curves.

So the name of the game is to compute some Gromov–Witten invariants. This can be done essentially geometrically using some homotopy-theoretic notions.

7 Finding Arithmetic Progressions in Dense Sets of Integers

This talk was given by Sarah Peluse. We are interested in finding arithmetic progressions. We will require our arithmetic progressions to have distinct terms. For example, we recall the following result from Ramsey theory.

Theorem 126 (van der Waeden)**.** For $k \geq 3$, and finite coloration of $\mathbb{N}$ has a monochromatic k-term arithmetic progression.

One could ask for more. Indeed, looking at these colorings, we know that at least one color has "the most" elements, so maybe that is the color with the progressions. To be precise, we need a notion of density.

Definition 127 (upper density)**.** For $A \subseteq \mathbb{N}$, we define the *upper density*

$$ud(A) := \limsup_{N\to\infty} \frac{1}{N}(A \cap \{1, \ldots, N\}).$$

The following was conjectured by Erdös and Turán.

Theorem 128 (Szmereédi)**.** If $A \subseteq \mathbb{N}$ has $ud(A) > 0$, then A contains a k-term arithmetic progression for any $k \geq 3$.

For example, $k = 3$ was shown by Roth via Fourier analysis and the circle method. Szmereédi proved this in 1975 via an elaborate combinatorial argument, using a regularity lemma in extremal graph theory.

By a compactness argument, this is equivalent to the following.

Theorem 129. Fix $k \geq 3$. Then the largest subset $A_N \subseteq \{1, \ldots, N\}$ with no k-term arithmetic progressions satisfies

$$\frac{|A_N|}{N} \to 0$$

as $N \to \infty$.

It is an open question to get an explicit rate of decay; for example, Szemédi is able to provide a (rather bad) asymptotic, something worse than arbitrarily many $\log$s. Even for $k = 3$, where Fourier analytic methods are availble, this remains a very active area of research. For example, we have been looking at $1/(\log N)^{1+\varepsilon}$ for some $\varepsilon \in (0, 1)$ for the past forty years, but in 2023, it was improved to $\exp(-c \sqrt[12]{\log N})$.

Gowers brought bounds past $k = 3$, introducing "higher-order Fourier analysis."

Theorem 130. If $A \subseteq \{1, \ldots, N\}$ contains no k-term arithmetic progressions, then

$$\frac{|A|}{N} \leq \frac{1}{(\log\log N)^{2^{-2^{k+9}}}}.$$

It was recently improved in 2024 to a bound like $\exp(C(\log\log N)^c)$.

Let's give a taste of the methods. For the remainder of the talk, instead of $\mathbb{Z}$, we will work in $\mathbb{Z}/p\mathbb{Z}$ for large p. Let $e_p \colon x \mapsto \exp(2\pi i x/p)$ be a character of G. The characters $\{e_p(ax) : a \in G\}$ form an orthonormal basis of the functions $G \to \mathbb{C}$. For example, there is a Fourier transform

$$\widehat{f}(x) = \sum_{\xi \in G} f(x) e_p(-\xi x),$$

there is some notion of Fourier inversion, and so on. For example, one can show identities like

$$\sum_{x,y\in G} f(x)g(x+y)h(x+2y) = \sum_{\xi\in G} \widehat{f}(\xi)\widehat{g}(-2\xi)\widehat{h}(\xi).$$

Letting $f = g = h = 1_A$ for some set A, we see that we are able to control the number of 3-term arithmetic progressions using $\widehat{1}_A$. For example, if we have large density α, then the number of arithmetic progressions is expected to be $\alpha^3 p^2$, so one expects a set A avoiding a 3-term arithmetic progression must have some other structure which we can utilize.

For longer progressions, it is harder to do much.

Example 131. The set B of elements n such that $\left\{\sqrt{2}n^2\right\} \in [0, 1/1000]$ has density about $1/1000$, but it has far more than $p^2/1000^4$ than one would expect because of some algebraic structure in B.

To replace the use of Fourier analysis for $k \geq 4$, we introduce higher-order Fourier analysis. Here are some definitions.

Definition 132. Given $f\colon G \to \mathbb{C}$, we define $\Delta_h f = f(x)\overline{f(x+h)}$ and $\partial_h g(x) = g(x) - g(x+h)$ to be discrete derivatives.

Definition 133. Given $f\colon G \to \mathbb{C}$ and $s \geq 2$, one has

$$\|f\|_{U^s}^{2^s} := \frac{1}{p^{s+1}} \sum_{x,h_1,\ldots,h_s \in G} \Delta_{h_1} \cdots \Delta_{h_s} f(x).$$

It is not obvious that this is well-behaved norm (e.g., is nonnegative), but it is true.

The important property of these norms is that they control k-term arithmetic progressions.

Lemma 134. Fix $A \subseteq G$ of density α. Then the number of k-term arithmetic progressions in A is about $\alpha^k p^2$, with error $\|1_A - \alpha\|_{U^{k-1}}$.

One shows this by applying Cauchy–Schwarz many times. It remains to study $f\colon G \to \mathbb{C}$ with $|f| \leq 1$ such that $\|f\|_{U^s}$ is large; this is called proving an "inverse theorem." Here is a sample, whose proof is elementary using the fact that $\|f\|_{U^2} = \left\|\widehat{f}\right\|_{\ell^4}$ (shown with some Fourier inversion).

Theorem 135. Choose $f\colon G \to \mathbb{C}$ with $|f| \leq 1$. Fixing $\delta \in [0,1]$, if $\|f\|_{U^2} \geq \delta$, then there is $\xi \in G$ such that $\left|\widehat{f}(\xi)\right| \geq \delta^2$.

Thus, we get some control of f: there is a large Fourier coefficient. Going back to A, this suggests that A should be close to an arithmetic progression. For $k = 4$, we need to bound U^3 norms. Roughly speaking, Gowers showed that having small U^3 means that one is close to some quadratic progression. For reasons related to nilsequences, it may still be difficult to find the needed 4-term arithmetic progression.

Without going into what a nilsequence is, we state the sort of result one gets from U^s bounds.

Theorem 136 (Green–Tao–Ziegler)**.** Let $f\colon G \to \mathbb{C}$ be a function with $|f| \leq 1$. Suppose $s \geq 2$ and $\delta \in [0,1]$. If $\|f\|_{U^s} \geq \delta$, then there is a reasonable nilsequence ψ such that

$$\left|\frac{1}{p} \sum_{x \in G} f(x)\psi(x)\right| \geq c(\delta, s).$$

Manners proved some qualitative bound for $c(\delta, s)$ (along the lines of Gowers), which look very reasonable. Leng, Sah, and Sawhney prove remarkably strong bounds (along the lines of an efficiency of Green, Tao, and Ziegler); their bounds are so good that it should improve techniques even for applications to primes.

8 L-Functions, Automorphic Forms, and Their Applications

This session happened on Saturday the 11th of January.

8.1 Central L-Values of the Cuspidal Asai Lifts

This talk was given by Wenzhi Luo.

Let's set up our Hilbert modular forms. For now, F is a real quadratic field over $\mathbb{Q}$ of narrow class number 1, and we write $\mathcal{O}_F$ for its ring of integers. Let σ_1 and σ_2 be the real embeddings. For an ideal $I \subseteq \mathcal{O}_F$, one can define a congruence subroup $\Gamma_0(I)$ in the usual way, and it acts on $\mathbb{H}^2$ by fractional linear transformations through σ_1 and σ_2.

Definition 137. A Hilbert modular form f of weight k is a holomorphic function satisfying the expected translation law

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} z\right) = \mathrm{N}(cz+d)^k f(z).$$

We let $M_k(\Gamma_0(I))$ denote the space of modular forms.

Because we have narrow class number 1, there is a Fourier expansion of the form

$$f(z) = \sum_{\alpha \in \mathcal{O}_F} a(\alpha) \exp(2\pi i \operatorname{tr}(\alpha z)),$$

where $a\colon \mathcal{O}_F \to \mathbb{C}$ is some coefficent function.

One can define cusps forms in $S_k(\Gamma_0(I))$ if it has no constant terms. For example, one can show

$$\dim_{\mathbb{C}} S_k(\Gamma_0(N)) \sim \frac{\operatorname{vol}\left(\Gamma_0(I)\backslash\mathbb{H}^2\right)}{(4\pi)^2}(k-1)^2.$$

There is also a Petersson inner product.

We now restrict to level $I = \mathrm{SL}_2(\mathcal{O}_F)$. There is also a notion of Hecke operators as before, so we can build some normalized Hecke eigenforms with Hecke eigenvalues $\lambda_f(\mu)$ for ideals $(\mu) \subseteq \mathcal{O}_F$, and we find that their L-functions

$$L(s,f) = \sum_{(\mu),\mu>0} \lambda_f(\mu)\,\mathrm{N}\,\mu^{-s}$$

have a behaved Euler product. The usual arguments also grant $L(s,f)$ a functional equation for a completed L-function $\Lambda(s,f)$ via some argument with theta series.

Asai defined a Dirichlet series of the type

$$L(s, \operatorname{As} f) \coloneqq \zeta(2s) \sum_{m=1}^{\infty} \lambda_f(m) m^{-s}.$$

One can use converse theorems to show that a completed L-function $\Lambda(s, \operatorname{As} f)$ admits a meromorphic continuation with prescribed poles and a functional equation. This thing also has an Euler product with local factors of degree 4. This can be viewed as a case of Langlands functoriality for $\operatorname{Res}\mathrm{GL}_{2,F} \to \mathrm{GL}_{4,\mathbb{Q}}$. Using the triple product, one can confirm that $\Lambda(s, \operatorname{As} f)$ is the L-function of an automorphic form of $\mathrm{GL}_{4,\mathbb{Q}}$.

We are interested in the behaviod of $L(s, \operatorname{As} f)$ on the critical line. Let's list some properties of L-functions of related constructions.

- Define $f^t(z_1,z_2) \coloneqq f(z_2,z_1)$, which one sees is still a Hilbert cusp form. Then the Rankin–Selberg convolution breaks down as

  $$L(s, f \otimes f^t) = L(s, \operatorname{As} f) L(s, \operatorname{As} f \otimes \chi_D),$$

  where χ_D is the Kronecker symbol modulo $D = \operatorname{disc} F$.

- If f is a base-change of a Hecke eigenform h from $S_k(\mathrm{SL}_2(\mathbb{Z}))$, then one can further factor
$$L(s, \operatorname{As} f) = L\left(s, \operatorname{Sym}^2 h\right) L(s, \chi_D).$$
Similarly, if f is a base-change from a Hecke eigenform $f \in S_k(\Gamma_0(D), \chi_D)$, then
$$L(s, \operatorname{As} f) = L\left(s, \operatorname{Sym}^2 h\right) \zeta(s).$$

We take a moment to give the following test for cuspidality of $\operatorname{As} f$.

Theorem 138. Fix everything as above.

(a) If f is non-dihedral, then $\operatorname{As} f$ is non-cuspidal if and only if f and f^t are twist-equivalent.

(b) If f is dihedral, then $\operatorname{As} f$ is non-cuspidal if and only if f is induced from a quadratic extension K of F which is biquadratic over $\mathbb{Q}$.

From here, we note that one can fix an orthogonal basis $\{f_j\}_j$ of Hecke eigenforms of $S_k(\mathrm{SL}_2(\mathcal{O}_F))$; for each j, we will write $\widetilde{f_j}$ for the normalized Hecke eigenform with first Fourier coefficient equal to 1. Then one can write out the Petersson formula for our Hilbert modular forms in terms of some generalized Kloosterman sums.

One can now use the above factorizations to get a bound on the coefficients $a_j(1)$ using the Rankin–Selberg method. Let's get our hands on the central value. One finds
$$L(1/2, \operatorname{As} f) = 2\sum_{n=1}^{\infty} \frac{\lambda_f(n)}{n^{1/2}} V_{1/2}\left(\frac{n}{\sqrt{D}}\right),$$
where $V_{1/2}$ is some volume term.

Theorem 139. Let $b\colon \mathcal{O}_F \to \mathbb{C}$ be a function on complex numbers defined modulo positive units. Then
$$\sum_j |L(1/2, \operatorname{As} f_j)| \ll k^{2+\eta},$$
where we restrict the sum to cuspidal Asai lifts.

These moments are better than one would expect for generic automorphic representations of GL_4.

Let's list some inputs to our result.

- One uses the formula for $L(1/2, \operatorname{As} f)$ to expand out the sum in terms of some Fourier coefficients.
- One uses the Petterson inner product formula to aid the bounding.
- Then one splits into cases between large and small level. In large level, there is not much to do. In the small level case, one reduces to the large level case using some embedding trick.

8.2 Lucas Congruences Using Modular Forms

This talk was given by Wei-Lun Tsai. Here is our prototypical result.

Theorem 140 (Lucas)**.** Fix nonnegative integers m and n. For a prime p,
$$\binom{n}{m} n \equiv \prod_{i=0}^{\infty} \binom{m_i}{n_i} \pmod{p},$$
where $\{m_i\}$ and $\{n_i\}$ are the base-p digits of m and n.

The moral of the story is that we can compute binomial coefficients in modular arithmetic quickly.

Proof. The idea is to use generating functions: note

$$\sum_{n=0}^{m}\binom{m}{n}X^n = (1+X)^m \equiv \prod_{i=0}^{\infty}\left(1+X^{p^i}\right)^{m_i} = \sum_{n=0}^{m}\left(\prod_{i=0}^{\infty}\binom{m_i}{n_i}\right)X^n.$$

By analogy, we have the following definition. ■

Definition 141 (Lucas congruence)**.** Fix a sequence $\{T(n)\}_{n\geq 0}$ to be an integer sequence with $T(0)=1$. This satisfies *Lucas congruence* $\pmod p$ for fixed prime p if and only if

$$T(n) \equiv \prod_{i=0}^{\infty} T(n_i)$$

where $\{n_i\}$ are the base-p-digits of n.

Remark 142. One really only has to check that $T(a+bp)\equiv T(a)T(b) \pmod p$ and then proceed inductively.

Example 143. For any $N>0$, one can take $T(n)=N^n$.

We would like a method to verify Lucas congruences. Here is another example.

Definition 144 (Apéry)**.** Define

$$A(n) := \sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}^2.$$

Theorem 145. The sequence $\{A(n)\}_{n\geq 0}$ satisfies the Lucas congruences.

Proof. Apply Lucas's original theorem. ■

Example 146. Because $A(0)$ and $A(1)$ are both odd, we see that $A(n)$ is always odd. Similarly, $3\nmid A(n)$ for all n.

Remark 147 (Rowland)**.** It also turns out that $A(n)\equiv A(p-1-n) \pmod p$ for all $n\in\{0,1,\ldots,p-1\}$.

Remark 148. It is conjectured that there are infinitely many p such that $p\nmid A(n)$ for all n. In fact, there is a conjectured density of these primes as $e^{-1/2}$. Roughly speaking, one uses the palindomic property and just guesses that the numbers from $A(0),\ldots,A((p-1)/2) \pmod p$ are chosen randomly and computes the limit as $p\to\infty$.

It turns out that one can relate these Apéry numbers to modular forms: there is an equation of the form

$$\sum_{n\geq 0} A(n)t(\tau)^n = Z(\tau)$$

where $t(\tau)$ and $Z(\tau)$ are some η-quotients. There is also a congruence

$$A\left(\frac{p-1}{2}\right) \equiv a(p) \pmod{p^2},$$

where the $a(p)$s are coefficients of a prescribed η-quotient.

Remark 149 (Malik–Straub)**.** It turns out that there are also "Apéry-like" sequences (due to Zagier) satisfying certain recursive relations similar to the Apéry numbers. These also satisfy the Lucas congruences, which one shows similarly upon giving an explicit summation.

Cooper has defined other Apéry-like sequences, but they do not all have closed forms. We will consider one of the form $T_{11}(n)$, which satisfies

$$\sum_{n\geq 0} T_{11}(n)t_{11}(\tau)^n = Z_{11}(\tau),$$

where t_{11} and Z_{11} are both an η-product divided by a theta series. One conjectures that this should satisfy Lucas congruences, and it has been checked in many cases. Here is our main result.

Theorem 150. The sequence $T_{11}(n)$ satisfies the Lucas congruences.

In fact, we show more; there is a generalization to other modular functions with level $\Gamma_0(N)$ and rather prescribed behavior (such as location of poles and zeroes). One can also allow $\Gamma_0(N)$ to be extended by a certain Atkin–Lehner involution of $\Gamma_0(N)$.

Let's give some inputs to the theorem.

- Let $E_k(\tau)$ be the Eisenstein series of even weight $k \geq 2$ and level $\mathrm{SL}_2(\mathbb{Z})$. Then there are congruences like $E_{2^m}(\tau) \equiv 1 \pmod{2^{m+1}}$ and $E_4(\tau) \equiv 1 \pmod{3}$.
- By considerations of the generating function, it really suffices to show a congruence of the form $Z(\tau) \equiv Z_{[p]}(t)Z(t^p) \pmod{p}$, where $Z_{[p]}$ is the truncation of the Taylor series up to the term τ^{p-1}.
- For $p \geq 5$, one defines

  $$G_p := \sum_d \left(E_{p-1}^2 | w_d\right) Z^{1-p},$$

  where the sum is over Hall divisors d of N (namely, we require $\gcd(d, N/d) = 1$). Thus, one finds that G_p is a modular function, and the prescribed behavior on Z yields prescribed behavior of G_p. Then one uses congruences for Eisenstein series to conclude.
- For $p \in \{2, 3\}$, one uses similar tricks. We remark that the $p = 2$ case requires quite a bit of care.

8.3 Relative Trace Formula and Automorphic L-Functions

This talk was given by Liyang Yang. Let's start with Brumer's conjecture. Let $J_0(q)$ be the Jacobian of the modular curve $X_0(q)$. Under the Grand Riemann hypothesis, Brumer showed

$$\mathrm{rank}_a\, J_0(q) \leq \left(\frac{3}{2} + o(1)\right) \dim J_0(q),$$

where rank_a is the analytic rank. This gives the following conjecture.

Conjecture 151 (Brumer)**.** One has

$$\mathrm{rank}\, J_0(q) \sim \frac{1}{2} \dim J_0(q).$$

Eventually, one was able to prove $\operatorname{rank}_a J_0(q) \leq c \dim J_0(q)$ without the grand Riemann hypothesis, and recently one has been able to take $c \approx 1.81$. Roughly speaking, the idea is that

$$L(s, J_0(q)) = \prod_{f \in S_2^*(q)} L\left(\frac{1}{2} + s, f\right),$$

so one wants to show

$$\operatorname{rank}_a J_0(q) = \sum_f \operatorname{ord}_{s=1/2} L(s, f) \leq c \# S_2^*(q).$$

This is some kind of nonvanishing problem. For example, one can show that about one-sixth of the f with $L(1/2, f) \neq 0$, which is enough to prove something.

In general, one can take a family $\mathcal{F}$ of automorphic representations and ask for

$$\liminf_{\# F \to \infty} \frac{\#\{\pi \in \mathcal{F} : L(1/2, \pi) \neq 0\}}{\#\mathcal{F}} \overset{?}{\geq} c$$

for an absolute constant c. For example, above we took $\mathcal{F} = S_k^*(q)$ as $q \to \infty$, but one can also consider Hilbert modular forms; one can also fix the level q and send $k \to \infty$. One can even consider other forms, such as Maass forms. There has been quite a bit of progress on such questions over the past few decades.

For now, we will fix a totally real field F of degree d and consider the set $\mathcal{F}(k, \mathfrak{q})$ of normalized Hilbert newforms over F of level $\mathfrak{q}$ and weight $k = (k_1, \ldots, k_d)$. One would like an explicit $C(k, \mathfrak{q}) > 0$ such that

$$\frac{\#\{\pi \in \mathcal{F}(k, \mathfrak{q}) : L(1/2, \pi) \neq 0\}}{\#\mathcal{F}(k, \mathfrak{q})} \geq C(k, \mathfrak{q}).$$

Here is our main result.

Theorem 152. Suppose $k_\bullet \geq 4$ always. For $\varepsilon > 0$ and A large enough, then

$$\frac{\#\left\{\pi \in \mathcal{F}(k, \mathfrak{q}) : L(1/2, \pi) > A^{-1}\right\}}{\#\mathcal{F}(k, \mathfrak{q})} \geq C(k, \mathfrak{q}, A).$$

In some families of As, one can also bound the $C(k, \mathfrak{q}, A)$s. Notably, this has been proven without the Grand Riemann hypothesis in a uniform way.

This is esssentially an application of Cauchy–Schwarz. Suppose we can estimate the two moments

$$\sum_{\pi \in \mathcal{F}(k, \mathfrak{q})} \frac{L(1/2, \pi)}{L(1/2, \pi, \mathrm{Ad})} \qquad \text{and} \qquad \sum_{\pi \in \mathcal{F}(k, \mathfrak{q})} \frac{L(1/2, \pi)^2}{L(1/2, \pi, \mathrm{Ad})}.$$

We do remark that the second moment is a bit problematic: one wants to use Kuznetsov's formula, but the error term there complicates the argument; one expects some error term like $O\left(n^{1/2+\varepsilon} k^{1/2+\varepsilon}\right)$ (because of microlocal analysis and the Gross–Zagier formula), but it seems difficult to actually achieve. Then the Cauchy–Schwarz inequality allows us to weed out and only sum over terms with $L(1/2, \pi) \neq 0$. Eventually, one is able to produce a bound of the form

$$\sum_{L(1/2, \pi) \neq 0} \frac{1}{L(1, \pi, \mathrm{Ad})} \geq \frac{c \cdot \#\mathcal{F}(k, \mathfrak{q})}{\log \#\mathcal{F}(k, \mathfrak{q})}.$$

There are now two things to fix: we need to get rid of the $\log$ and get rid of the $L(1, \pi, \mathrm{Ad})$.

Let's describe how one removes the $\log$ term. The idea is to then bound the twisted moments

$$\sum_{\pi \in \mathcal{F}(k, \mathfrak{q})} \frac{\lambda_\pi(\mathfrak{n}) L(1/2, \pi)}{L(1/2, \pi, \mathrm{Ad})} \qquad \text{and} \qquad \sum_{\pi \in \mathcal{F}(k, \mathfrak{q})} \frac{\lambda_\pi(\mathfrak{n}) L(1/2, \pi)^2}{L(1/2, \pi, \mathrm{Ad})},$$

where $\lambda_\pi(\mathfrak{n})$ is the Hecke eigenvalue. (One needs to do some "mollification" to get everything done.) Then one can average over the $\lambda_\pi(\mathfrak{n})$s to eventually get rid of the $\log$.

Let's provide a bit more detail on the second moment. We now explain how to use the relative trace formula. A nice function f on $\operatorname{PGL}_2(F)\backslash\operatorname{PGL}_2(\mathbb{A}_F)$ allows us to define a kernel

$$K(g_1,g_2)=\sum_{\gamma\in\operatorname{PGL}_2(F)}f\left(g_1^{-1}\gamma g_2\right).$$

On the other hand, there is a specrtal expansion of K as

$$\sum_\pi\sum_\phi\lambda_\pi(\mathfrak{n})\phi(g_1)\overline{\phi(g_2)}.$$

Then one evalautes an average of K and compares the spectral and geometric sides. One gets out the second moment from the spectral side, and from the geometric side, we find that the error term is given by some orbitral integral. This orbitral integral turns into some local Bessel functions, which can be bounded.

It remains to prove the $L(1,\pi,\operatorname{Ad})$ weight. This is essentially a standard technique due to Kowalski–Michel, but one needs to be careful with the mollifier to get the needed bounds.

There is also a general case for higher-rank groups. A nice function $f\colon G(\mathbb{A}_F)\to\mathbb{C}$ defines an intertwining operator $R(f)$ by integrating against a kernel K defined via f. Then one again has a relative trace formula. Approximately speaking, one then hopes to get the geometric side to have some Rankin–Selberg L-functions and some special functions on F^n. The spectral side features the desired central values of Rankin–Selberg L-functions. Here is a taste for what we can prove.

Theorem 153. There are infinitely many automorphic representations π of $\operatorname{PGL}_{3,F}$ such that

$$L(1/2,\pi\times\chi)L(1/2,\pi\times\sigma)\neq 0,$$

where χ is a unitary Hecke character, and σ is a unitary cuspidal automorphic representation of $\operatorname{GL}_{2,F}$.

With some work, it is also possible to give a quantitive bound on how many π there are.

8.4 The Subconvexity Problem for Rankin–Selberg L-Functions

This talk was given by Junxian Li. Let f be a primitive cusp form of level q and central character χ_f, and let g be a Hecke eigenform of level D and central character χ_g. If $\gcd(q,D)=1$, one can define a Rankin–Selberg $L(s,f\otimes g)$ by directly multiplying the coefficients. It admits a meromorphic continuation with controlled poles, and there is a completed L-function $\Lambda(s,f\otimes g)$ with some functional equation.

Now, the Phragmen-Lindelöf principle produces a convexity bound

$$L(s,f\otimes g)\ll\mathfrak{q}(s,f\otimes g)^{1/2+\varepsilon},$$

where $\mathfrak{q}(s,f\otimes g)$ is some analytic conductor; this conductor grows like q^2 times some polynomial in the weight of f.

The subconvexity problems asks us to give a $\delta>0$ with a bound

$$L(s,f\otimes g)\overset{?}{\ll}\mathfrak{q}(s,f\otimes g)^{1/2-\delta},$$

where f varies with fixed g. For example, this has applications to equidistribution of points on Shimura curves and bounds on the number of Fourier coefficients needed to distinguish between modular forms. This problem was solved essentially completely over about fifteen years by many authors (Duke, Friedlander, Iwaniec, Kowalski, Michel, Harcos, and Venkatesh).

The general approach is to estimate the second moment

$$\sum_{f\in\mathcal{F}}|L(1/2,f\otimes g)|^2\left|\sum_{\ell\leq L}\lambda_f(\ell)x_\ell\right|^2,$$

where the right-hand term is an amplifier intended to focus the contribution. Then one uses a Petersson or Kuznetsov formula to sums of Kloosterman sums, and then one uses some spectral theory of automorphic forms. We remark that the need for this spectral theory means that subconvexity bounds are mostly only available in low degree, though there are some things known.

There is another "delta" approach due to Munshi. It was able to work with general automorphic forms attached to GL_3, and it is able to achieve better exponents in subconvexity. Here is the sort of thing we are able to prove.

Theorem 154. Fix a prime p, and let f be a primitive cusp form of level p and with central character $\chi_f \pmod{p}$. Further, let g be a Hecke eigenform of level 1. Then we have

$$L(1/2, f \otimes g) \ll_g p^{1/2-1/524+\varepsilon}.$$

For example, this is uniform in f (among modular and Maass forms), and the bound is independent on the progress towards the Ramanujan conjecture. Notably, we do not use the spectral theory of automorphic forms.

Instead, we will use bounds of the form

$$\sum_{\gcd(m,n)=1} \alpha_m \beta_n e\left(\frac{am}{n}\right) \ll \|\alpha\| \, \|\beta\| \, (|a| + MN)^{3/8}(M+N)^{11/48+\varepsilon}$$

due to Duke–Friedlander–Iwaniec. Roughly speaking, this can be considered a bilinear form on Kloosterman sums, though we note that there is technology now to get savings on trilinear forms, due to Bettin and Chandee.

Let's sketch some ideas that go into the proof.

1. Using the functional equation, it essentially suffices to produce an estimate like

$$S(N) := \sum_{n \approx N} \lambda_f(n)\lambda_g(n) \ll \sqrt{N} p^{1/2-\delta},$$

for some $\delta > 0$.

2. One needs to apply an amplification to $S(N)$ as follows. Given $L \geq 1$, we define γ_ℓ to be 1 if prime about the size of L, and it is zero otherwise. Then we apply some scaling to $S(N)$.

3. The delta method then separates f and g using some kind of circle method. Roughly speaking, the idea is that one can detect $n = 0$ with the sum

$$\frac{1}{C^2} \sum_{c \leq c} \sum_{h \pmod{c}} e_c(hn),$$

where $C = \sqrt{n}$ and $e_c(x) = \exp(2\pi i x/c)$. One plugs this into our amplified $S(N)$ to separate f and g.

4. Some Voronoi summation reduces the length of the sum.

5. Lastly, one applies the Cauchy–Schwarz inequality, some Poisson summation, and exponential sums. The Duke–Friedlander–Iwaniec inequality given above is applied to these exponential sums.

From here, one hopes to be able to handle other levels or maybe achieve some uniformity in g.

8.5 Second Moment of $\mathrm{GL}(3)$ L-Functions

This talk was given by Wing Hong Leung. As usual, we note that the Riemann ζ-function has a Dirichlet series, Euler product, meromorphic continuation with prescribed poles, and funcitonal equation, and such a thing typically has an unproven Riemann hypothesis. An L-function is a generalization including all the previous properties.

Today, we are focusing on L-functions for $\mathrm{GL}_{3,\mathbb{Q}}$. The Dirichlet series

$$L(s,f)=\sum_{n\geq 1}\lambda(1,n)n^{-s}$$

converges in the region $\{s:\operatorname{Re}s>2\}$.

Example 155. For example, if $f=1\boxplus 1\boxplus 1$, then $L(s,f)=\zeta(s)^3$.

We are interested in bounding

$$\int_T^{2T}\left|L(1/2+it,f)\right|^3\,dt.$$

The "trivial" bound is $T^{3/2}$. For example, if $L=\zeta^3$, then this is the sixth moment of ζ. After expanding out this sum, the point is to estimate some shifted sum

$$S(N,H)=\sum_{h\approx H}\sum_{n\approx N}\lambda_f(n)\lambda_f(n+h),$$

where $N\ll T^{3/2}$ and $H\ll\sqrt{T}$.

Currently, the asymptotics are wide open, but there is an upper bound of $T^{5/4+\varepsilon}$ by interpolating the fourth moment and the twelth moment. Here is the sort of thing that we have been able to show.

Theorem 156. One has

$$\int_T^{T+T^{2/3}}\left|L(1/2+it,f)\right|^2\,dt\ll_\varepsilon T^{5/4+\varepsilon}.$$

Remark 157. By a decomposition idea, this was used to achieve the bound

$$\int_T^{2T}\left|L(1/2+it,f)\right|^2\,dt\ll_\varepsilon T^{3/2-3/88+\varepsilon}.$$

The main result of the talk is as follows.

Theorem 158. One has

$$\int_T^{2T}\left|L(1/2+it,f)\right|^2\,dt\ll_\varepsilon T^{4/3+\varepsilon}.$$

As one would expect, one really achieves a bound on $S(N,H)$ of the form $N^{4/3+\varepsilon}H^{-1/3}+\cdots$.

Let's give a few applications. For example, we are of course going to achieve a subconvexity bound (on average). There is an application to the Rankin–Selberg problem trying to achieve a bound

$$\sum_{n\leq X}\left|\lambda_g(n)\right|^2=c_gX+O_{g,\varepsilon}\left(X^{3/5-\delta+\varepsilon}\right)$$

for some $\delta<0$. By using $f=\operatorname{Sym}^2 g$ with our L-function bound, we are able to take $\delta=1/35$. We also mention that one can bound central values for things like $\operatorname{Sym}^3 g$.

Let's sketch the argument.

Remark 159. The only $\mathrm{GL}(3)$ ingredient that we will need Voronoi summation to show that the sums of the coefficients are something like $O(1)$.

Choose a weight function V. Because we are not interested in asymptotics, we may as well bound

$$\int_{\mathbb{R}} V\left(\frac{t}{T}\right)\left|L\left(\frac{1}{2}+it,f\right)\right|^2\,dt.$$

Using the approximate functional equation, one can bound $L(1/2+it,f)$ by a sum of $N^{-1/2}\sum_{n\approx N}\lambda(n)n^{-it}$ for N of the size $T^{3/2}$.

Now, opening up the square and integrating, one eventually finds that we are approximately

$$\frac{1}{\sqrt{T}}\sum_{|h|\approx T^{1/2}}\sum_{n\approx T^{3/2}}\lambda(n)\overline{\lambda}(n+h),$$

which explains how we got to a shifted sum. We now focus on bounding the shifted sum.

We now apply the delta method. The point is to replace $\lambda(n+h)$ with a sum over $\lambda(m)\delta(m=n+h)$ and then replace $\delta(m=n+h)$ with an exponential sum

$$\frac{1}{Q^2}\sum_{q\le Q}\sum_{a\pmod q}e\left(\frac{an}{q}\right)U\left(\frac{n}{qQ}\right),$$

where Q is an even smooth function with $U(0)=1$. The point is that we have smoothly decomposed the indicator into harmonics, which will eventually let us produce a bound without having to think about shifted sums. We will take Q to be about $T^{7/12}$, which we think about as a conductor-lowering trick.

The moral of the story is that we have separated m and n and h. Applying some standard tricks (Poisson summation, Voronoi summation, Mellin inversion) allows us to continue. Eventually we get to something that looks like

$$\int\sum_q\sum_h\left|\sum_n\lambda(n)S(\overline{h},n;q)n^{iy}\right|^2\,dy.$$

One can try to apply the large sieve directly, but it does not work well because the sums are not similar in size. Instead, we will apply a duality principle, which lets us move the long n size outside and move the integral and sum over q inside the absolute values. With the long sum outside, we open up the square and apply Poisson summation. There were many other steps, which I got too tired to record.

8.6 On Higher Regulators of Picard Modular Surfaces

This talk was given by Linli Shi, and it is about arithmetic geometry.

We begin by introducing Bellinson's conjecture on special values. We are interested in special values of motivic L-functions generalizing the class number formula relating a special value to some regulator (along with some other data). Let's explain how to generalize this regulator. Fix a smooth projective variety X over $\mathbb{Q}$, and choose $i\geq 0$ and some integer n with $2n>i$. We are now interested in the motivic cohomology group $H^{i+1}_M(X,\mathbb{Q}(n))$. For example, if $2n=i+1$, then we are looking at a Chow group. There is also an absolute Hodge cohomology.

Now, let M be a pure motive of the form $h^i(X)(n)$, and we can define a motivic L-function $L(M,s)$. For example, we recall that there is an Euler product for $\operatorname{Re}s>1+w/2$ using the Weil conjectures; it is only conjectured that there is a meromorphic continuation and functional equation. There is still a notion of completed L-function, for which we use some Hodge theory to build a Gamma factor $\Gamma_\infty(M,s)$; some $n\in\mathbb{Z}$ is called critical if and only if it is a pole of $\Gamma_\infty(M,s)$ (or $\Gamma_\infty(M,w+1-s)$).

Deligne then conjectured that

$$L(m,0)\in c^+\mathbb{Q}^\times,$$

where $c^+(M)$ is called the Deligne period, and it is defined using Hodge theory. On the other hand, Bellinson conjectured that (when $s=0$ is non-critical and some technical condition)

$$L(M,0)\mathcal{D}(M)\equiv\wedge^{\text{top}}r_H(H^{i+1}_M(X,\mathbb{Q}(n))),$$

where r_H is a regulator map, and $\mathcal{D}(M)$ is a Deligne rational structure also defined using Hodge theory.

For our main result, we will want some notions. Let E be an imaginary quadratic field of discriminant $-D$, and let $x \mapsto \overline{x}$ denote complex conjugation. We will work with the group $\mathrm{GU}(2,1)$. Our motives of interest will come from Picard modular surfaces, which are generalizations of modular curves. They are Shimura surfaces defined over E, essentially given by taking the quotient of the complex ball

$$X = \{(z_1, z_2) : |z_1|^2 + |z_2|^2 \leq 1\}$$

by some arithmetic group.

Lastly, for a cusp form, we recall that there is a Grothendieck motive $M(f)$. This story is known over GL_2, which is why we are working with $\mathrm{GU}(2,1)$. Now, f gives rise to an automorphic form π of $\mathrm{GU}(2,1)$, and π also a Grothendieck motive. So our main result is to prove Bellinson's conjecture in this case. The general steps to prove such thing are as follows; let S e the Shimura variety of $G = \mathrm{GU}(2,1)$, and we let M be the Shimura variety of H.

1. One constructs some motivic classes.
2. Then one proves that the onstructed classes live in a controlled subspace.
3. Lastly, one computes the image of these motivic classes along r_H.

So the main result is some version of Bellinson's conjecture, which had a fairly technical statement.

8.7 Adelic Distributions and Euler Systems for $\mathbb{Z}_p(1)$

This talk was given by John Jae Hyung Sim. My computer is about to die, so I will not take notes.

9 Current Directions on Modular Forms

This session happened on Saturday the 11th of January.

9.1 Modular Functions and the Monstrous Exponents

This talk was given by Holly Swisher. As usual, modular functions are meromorphic functions $f \colon \mathbb{H} \to \mathbb{C}$ which is invariant under the action of some subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$. If, we assume $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma$, then one gets the usual q-expansion; for example, the modular j-function can be given a q-expansion. For motivation, we recall that the j-function provides a biholomorphic function $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^* \to X_0(1)$ so that $j(\tau)$ is the j-invariant of the elliptic curve $(\mathbb{Z} + \mathbb{Z}\tau)\backslash\mathbb{H}$.

Suppose that Γ produces a modular form $X_0(\Gamma)$ of genus 0. Then we may look for a Hauptomodul, which is the biholomorphic function satisfying the properties of the previous paragraph. It is desirable to have a Hauptomodul with vanishing constant term, so we will define $J_1(z) := j(z) - 744$.

Let's recall something about moonshine. There is a coefficient 196884 of the j-function, and 196883 is an irreducible representation of the monster group M. Conway and Norton conjectured the existence of an infinite graded representation

$$V^\natural \overset{?}{=} \bigoplus_{n \geq -1} V_n^\natural$$

so that each $g \in G$ has

$$\sum n \geq -1 \operatorname{tr}(g|V_n^\natural) q^n$$

produces a Hauptomodul of the normalizer Γ_g. In 1984, we were able to construct $V^\natural$ so that

$$J_1(\tau) = \sum_{n \geq -1} \dim V_n^\natural q^n,$$

completing the $g = 1$ case. The conjecture of Conway and Norton was finally proven by Borcherds in 1992, from which he won a Fields medal.

Even before we had any moonshine, Ogg noticed that $p \mid \#M$ if and only if $X_0(p)^+$ has genus 0 (where $\Gamma_0(p)^+$ is $\Gamma_0(p)$ along with $p^{-1/2}\left[\begin{smallmatrix} & -1 \\ p & \end{smallmatrix}\right]$), which is equivalent to the primes p so that the supersingular j-invariants are defined over $\mathbb{F}_p$. In 2015, Duncan and Ono showed that each $p \mid \#M$ has a conjugacy class "p^+" of elements of M of order p so that

$$\sum_{n\geq -1} \operatorname{tr}(g|V_n^\natural)q^n$$

is a Hauptomodul for $\Gamma_0(p)^+$, which we call J_{p^+} after removing the constant term. They showed $J_{p^+} - J_1 = J_{p^+}|U_p$. They then showed that $J_{p^+}|U_p$ is equivalent to some weight $(p-1)$ modular form f taken $\pmod p$. This does something to explain the primes dividing the monster.

We would like to also explain the exponents of the primes $p \mid \#M$. We divide into cases.

1. If $\Gamma_0(p)^+$ has genus 0 but $\Gamma_0(p)$ has genus ≥ 1, then M has only one conjugacy class of p-power order, which is the p^+ above. This corresponds to this subgroup $\Gamma_0(p)^+$.
2. If $\Gamma_0(p)^+$ and $\Gamma_0(p)$ have genus 0 but $\Gamma_0(p^2)$ have genus at least 1. Then there are two conjugacy classes of p-power order, named p^+ and p, and they correspond to $\Gamma_0(p)^+$ and $\Gamma_0(p)$.
3. Otherwise, there are lots of conjugacy classes.

We are able to exlpain the exponents seen in the first two cases. Here is a taste.

Theorem 160. If p is a prime in the first case, then

$$\nu_p(\#M) = \nu_p(J_1 - J_{p^+}).$$

There is a similar result for the second case and even $p = 5$. It remains to work out $p \in \{2, 3\}$.

Let's say something about the proof in the first case, other than 11.

- Following Duncan and Ono, there is a replicability property which yields
$$J_1(\tau) - J_{p^+}(\tau) = \sum_{k=0}^{p-1} J_{p^+}\left(\frac{\tau+k}{p}\right).$$
Then one can give the right-hand side a q-expansion.
- Deligne explained how to split up $J_1|U_p$ in terms os supersingular j-invariants taken $\pmod p$.
- The point then is that one can find some term not divisible by p, allowing us one to show something like $J_{p^+}|U_p \not\equiv 0 \pmod p$.

9.2 Replicable Functions Arising from Towers

This talk was given by Stephanie Treneer. Rougly speaking, codes go to lattices go to vertex operator algebras. Each has an associated automorphism group and a counting function (weight enumerator, theta function, and character, respectively).

Example 161. By way of motivation, there is a "moonshine tower" consisting of the Golay code $\mathcal{G}$, which then constructs the Leech lattice Λ_{24}, which constructs the moonshine vertex operator algebra. And one can track through the automorphism groups and counting functions. For example, the automorphism groups are M_{24} (the Matthieu group), Co_0 (the Conway group), and M, respectively.

For today, we will mostly work with lattices and codes.

Definition 162. A *bilinear linear $[n,k]$-code* is a k-dimensional subspace $C \subseteq \mathbb{F}_2^n$; an element is a codeword. We say C is *doubly even* if and only if the weights of all the codewords are divisible by 4.

For example, there are Hamming codes and a Golay code.

Lattices are as usual. All of our lattices will be even, unimodular, and positive-definite. It turns out that these produces codes and lattices of ranks divisible by 8. For example, at rank 8, there is only the lattice E_8. For rank 16, there are two lattices, but there are many more as the rank increases.

Let's take a code C and construct a lattice. Begin with the standard basis $\{\alpha_i\}$ of $\mathbb{R}^n$ each scaled by $\sqrt{2}$. Then for each $b \in C$, we define

$$\alpha_B \coloneqq \sum_{\substack{1 \le i \le n \\ b_i = 1}} \alpha_i.$$

Then $L(C)$ is the lattice of $\frac{1}{2}\alpha_B + L'$ where $L' = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$.

To compute some automorphisms, we note that S_n permuts C on the coordinates, and we can ask for automorphisms which preserve C. These are put into $\operatorname{Aut}(C)$. It turns out that there is an embedding $\iota\colon \operatorname{Aut} C \to \operatorname{Aut} L(C)$, which is the subset of automorphisms of interest to us. Notably, for each $g \in \operatorname{Aut} L$ coming from a code automorphism, it is fairly easy to explicitly write down the set of fixed points in L^g in terms of some combinatorics of the cycle type of $g \in S_n$. One can work with fixed sublattices like L^G for more general subgroups $G \subseteq \operatorname{Aut} C$.

We are now ready to define our theta functions. Define

$$\theta_L(z) \coloneqq \sum_{\lambda \in L} q^{\langle \lambda, \lambda \rangle / 2}.$$

Because of the hypotheses on our lattice of rank n, we produce a modular form of weight $n/2$. We would like to compute theta functions of fixed sublattices. One expects to recover "replicable" functions. For example, it turns out that the functions

$$T_g(\tau) = \sum_{n \ge -1} \dim V_n^\natural q^n,$$

where $V^\natural$ is the Moonshine vertex operator algebra, satisfy some replication formula

$$\sum_{ad=n} T_{g^a}\left(\frac{\tau + a}{n}\right)$$

being equal to some prescribed polynomial. This motivates the following definition.

Definition 163. Write $f(q) = \frac{1}{q} + \sum_{m \ge 1} a_m q^m$. Then f is *replicable* if and only if

$$\sum_{ad=n} f_a\left(\frac{a\tau + b}{d}\right)$$

is some prescribed Faber polynomial.

Previous work took sublattices of the Leech or E_8 lattices and found some nice functions.

The main results of the talk find some theta functions built from L^G for subgroups $G \subseteq \operatorname{Aut} C$.

Theorem 164. Fix everything above. Then

$$\left(\frac{\theta_{L^G}(q)}{\eta_G(q)}\right)^{24/N}$$

is a weakly holomorphic modular function.

For example, one can write out all the computation and find that 19 of the 65 conjugacy classes from E_8 produce replicable functions. One is also able to find that certain replicable functions appear many times.

9.3 Rational Torsion Points on Abelian Surfaces with Quaternion Multiplication

This talk was given by John Voight. It was in the session on quaternions. For now, quaternions will act by endomorphisms on our abelian surfaces. We are interested in torsion of such abelian surfaces.

Let's recall some facts from elliptic curves. For an elliptic curve E over $\mathbb{Q}$, we can write $E(\mathbb{C})$ has $\mathbb{C}/\Lambda$ for a lattice Λ. Its m-torsion is then isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$ all defined over $\overline{\mathbb{Q}}$. Sometimes an elliptic curve has complex multiplication, which means that there is an "unexpected" endomorphism. For example, the equatino $y^2 = x^3 + 1$ has an endomorphism $(x, y) \mapsto (\zeta_3 x, y)$. Over $\mathbb{Q}$, there is a classification of torsion.

Theorem 165 (Mazur)**.** An element $p \in E(\mathbb{Q})$ of torsion order ℓ, then $\ell \leq 7$.

We are far from a result like Mazur's for general abelian varieties. There are results for complex multiplication which are older. For today, we will turn to quaternionic multiplication, meaning that our abelian surface A over $\mathbb{Q}$ has $\operatorname{End}(A_{\overline{\mathbb{Q}}})_{\mathbb{Q}}$ containing a quaternion algebra. For example, one can find explicit genus-2 curves with quaternionic multiplication. We note also that there are compact Shimura curves parameterizing these, which motivates us thinking about these things similarly to elliptic curves.

Here is an example theorem.

Theorem 166. Suppose A is an absolutely simple abelian surface with potential quaternionic multiplication by a maximal order. Then the torsion of prime order has order 2 or 3.

One can then classify possible torsion groups, though we have some torsion groups where we do not know if they actually exist or not, but for about half of the groups, we have found at least one Shimura curve parameterizing them.

By way of example, let's work with $\mathbb{Z}/4\mathbb{Z}$. For example, we can work with the family of curves

$$C_t \colon y^2 = x^5 + 8x^4 + tx^3 + 16x^2 - 4x.$$

This family was found by interpolation when building the database. (Namely, they found all these examples for given t and then guessed the result.) Here, the quaternion algebra is given by $B = \operatorname{span}_{\mathbb{Q}}\{1, i, j, k\}$ with $i^2 = -1$ and $j^2 = 3$, which has discriminant 6. Then $\operatorname{Jac} C_t$ has potential quaternionic multiplication by a non-maximal order in B. For some special values of t, one can find an isogeny $\operatorname{Jac} C_t \to A_t$ of degree 2, and now A_t has potential quaternionic multiplication by a maxial order of B. (However, A_t fails to be principally polarized!) It turns out that $\mathbb{Z}/4\mathbb{Z} \subseteq A_t(\mathbb{Q})_{\text{tors}}$ for all but finitely many t.

9.4 Zeros of Partition-Theoretic Polynomials

This talk was given by Larry Rolen. Let's study the partition function $p(n)$. Hardy and Ramanujan proved some asymptotic of the form

$$p(n) \sim$$

There are also some Ramanujan congruences such as $p(5n+4) \equiv 0 \pmod 5$, and one can use Tate cycles to show that $\{5, 7, 11\}$ are the only congruences which look like this. In general, the idea is to put these things in generating functions and see what comes out.

For now, we will be interested in polynomials, which we view as "finite" generating functions. Here is an example.

Definition 167. For a real sequence $\{a(n)\}_{n \geq 0}$, the degree d and shift n Jensen polynomial is

$$J_a^{d,n}(X) := \sum_{j=0}^{d} a(n+j)\binom{d}{j} X^j.$$

Definition 168 (log concave)**.** A sequence $\{a(n)\}_{n\geq 0}$ is *log concave* if and only if $a(n)a(n+2) \geq a(n+1)$.

Then one can use these polynomials $J_p^{2,n}$ only having real roots (eventually) to show the following.

Theorem 169 (DeSalvo–Pak)**.** The partition function is log concave for $n \geq 26$.

There are other inequalities that one is able to show by showing that eventually $J_p^{d,n}(X)$ has all real roots. This is one of main theorems.

Theorem 170. There is $N(d)$ where $J_p^{d,n}(X)$ has real roots for all $n \geq N(d)$.

It is an observation of Don Zagier that one can relate these functions to Hermite polynomials. The moral is that we gained analytic knowledge of partitions by studying zeroes of some special orthogonal polynomials.

Let's think about congruences next.

Definition 171. Define $\operatorname{rank}(\lambda)$ of a partition λ is the largest part minus the number of parts. We will let $N(m,n)$ be the number of partitions of n with rank m, and we let $N(m,q,n)$ be the number of partitions of n with rank equivalent to $m \pmod q$.

Then one finds a generating function

$$\sum_{m,n\geq 0} N(m,n)\zeta^m q^n,$$

which turns out to be a mock modular form. Then one can prove something about this generating function, which turns out to come from a polynomial divisibility of the form

$$\Phi_5(\zeta) \mid \left[q^{5n+4}\right] R(z;\tau).$$

One may want a bijective proof of this, which suggests the existence of some modular object underneath. We were able to use polynomial techniques to prove these sorts of things as well.

Remark 172. Recently, there has been a drive to look at various partition functions and look for patterns in the roots. This was a little fast, so I didn't write these examples out.

9.5 Automorphic Form Twisted Adelic Shintani Functions

This talk was given by Eun Hye Lee. Let's define the Shintani zeta function. Fix a commutative ring R. Then we may let V_R denote the space of binary cubic forms $ax^3+bx^2y+cxy^2+y^3$, and we note that $\mathrm{GL}_3(R)$ acst by coordinate changes. We note that $V_\mathbb{R}$ and $V_\mathbb{C}$ are prehomogeneous spaces when equipped with that action.

Now, define $\widehat{V}_\mathbb{Z}$ to consist of the $f \in V_\mathbb{Z}$ with $3 \mid b, c$. We are now ready to define the Shintani zeta function

$$\xi^\pm(s) := \sum_{x\in \mathrm{SL}_2(\mathbb{Z})\backslash V_\mathbb{Z}} \frac{1}{|\mathrm{Stab}(x)|} \left|\mathrm{Disc}(x)\right|^{-s}.$$

Their importance arises because $\xi^\pm(s)$ is the generating function for the number of cubic rings. Shintani proved an analytic continuation (as a vector (ξ^+,ξ^-)) along with a functional equation; however, there is no Euler product, and it fails any form of the Riemann hypothesis.

Now, for a cusp form ϕ, we define the twist $\mathcal{L}_\pm(s,\phi)$, and one can show something similar for Eisenstein series. Then one has a meromorphic continuation with prescribed poles and functional equation.

Theorem 173. The twists $\mathcal{L}$ by twists of Hilbert modular forms admit meromorphic continuation with prescribed poles and a functional equation.

One shows this adelically by finding an integral representation like

$$Z(\omega, \Phi, \varphi) \coloneqq \int_{\mathrm{GL}_{2,\mathbb{A}} \backslash \mathrm{GL}_{2,k}} \omega(\det g)\varphi(g) \sum_{x \in V_k'} \Phi(gx)\, dg,$$

where ω is a character, Φ is a Schwarz test function (vanishing on the zero locus of the discriminant), and φ is either a cusp form or an Eisenstien series. One then proceeds as in Tate's thesis. The speaker worked out the proof in the slides, but I did not record it.