Berkeley Undergraduate Number Theory Talks

Nir Elber

August 2022

Contents

1 Thin Sets of Primes — Yunqing Tang

Yunqing Tang did math olympiad contests in high school, chose to do math in college, did a reading course on complex projective varieties, went to grad school at Harvard, did a postdoc at Princeton, and she is now at Berkeley.

Today we're going to talk about elliptic curve and some curves of higher genus.

1.1 Sato–Tate for Fun and Profit

We are interested in studying integer solutions to equations $P(x,y)=0$ for polynomials $P\in\mathbb{Z}[x,y]$.

Example 1. Consider the degree-2 equation $x^2+1=0$. There are no real solutions, but there are solutions $\pmod p$ for some primes p. Here is a table with primes p and the number of solutions $N(p)$ to $x^2+1=0$ in $\mathbb{F}_p$.

p	2	3	5	7	11	13	$\cdots$
$N(p)$	1	0	2	0	0	2	$\cdots$

It turns out that $p=2$ has $N(p)=1$, and $p\equiv 1 \pmod 4$ has $N(p)=2$, and $p\equiv 3 \pmod 4$ has $N(p)=0$.

Example 2. Consider the degree-3 equation $y^2=f(x)$ (here, f is a cubic), where the discriminant of $f(x)\neq 0$; i.e., we require that $f(x)$ has no repeated roots in $\mathbb{C}$. To be concrete, let's look at

$$y^2+y=x^3-x^2-10x-20.$$

(To put this in the form $y^2=f(x)$, one should complete the square on the left-hand side, but this introduces problems at $p=2$.) Heuristically, we expect $y^2=f(x)$ to have p solutions $\pmod p$ because each value of $x\in\mathbb{F}_p$ has an expected value of 1 solution to $y^2=f(x)$. To measure the error, we set $a_p\coloneqq N(p)-p$, where $N(p)$ is the number of solutions over $\mathbb{F}_p$. Here is the table.

p	2	3	5	7	11	13	17	19	$\cdots$
a_p	-2	-1	1	-2	1	4	-2	0	$\cdots$

Remark 3. It turns out that the a_p are Fourier coefficients of a weight-2 cusp form associated to $X_0(11)$; this remark comes from the Modularity Theorem.

Motivated by Example 2, we might want to know how frequently our guess of $a_p=0$ is correct on the nose. Sadly, we have the following.

Theorem 4 (Serre)**.** Fix an elliptic curve $y^2=f(x)$, and set $a_p\coloneqq p-N(p)$ where $N(p)$ is the number of solutions in $\mathbb{F}_p$. Then we have the density result

$$\lim_{X\to\infty}\frac{\#\{\text{prime } p<X : a_p=0\}}{\#\{\text{prime } p<X\}}=\begin{cases}1/2 & \text{if } E \text{ is CM},\\ 0 & \text{else.}\end{cases}$$

Here, an elliptic curve "is CM" or "has complex multiplication" if and only if it has automorphism ring larger than $\mathbb{Z}$.

Example 5. The elliptic curve $y^2=x^3+1$ has CM. In addition to the endomorphisms coming from $\mathbb{Z}$, there is the map $(x,y)\mapsto(\zeta_3 x,y)$, which gives us endomorphism ring $\mathbb{Z}[\zeta_3]$.

One might ask why we could expect this result.

Remark 6. Fix an elliptic curve $y^2=f(x)$, and define a_p as usual. It is a result due to Hasse that $|a_p|\le 2\sqrt{p}$. Roughly speaking, a_p measures the trace of some two-dimensional operator, and one can show that this operator has eigenvalues of absolute value less than or equal to $\sqrt{p}$.

The remark tells us that we should normalize a_p to $a_p/\sqrt{p}$.

Theorem 7 (Sato–Tate)**.** Fix a non-CM elliptic curve $y^2 = f(x)$. Then the distribution of $a_p/\sqrt{p} \in [-2, 2]$ is essentially a semicircle: for $-2 \le a < b \le 2$, one has

$$\lim_{X\to\infty} \frac{\#\{\text{prime } p < X : a_p/\sqrt{p} \in [a,b]\}}{\#\{\text{prime } p < X\}} = \int_a^b \sqrt{4-t^2}\,dt.$$

For example, one can heuristically compute the probability of $a_p = 0$ as the probability of $-1/\sqrt{p} < a_p/\sqrt{p} < 1/\sqrt{p}$, so one has

$$\operatorname{Prob}\left(a_p/\sqrt{p} \approx 0\right) \approx 1/\sqrt{p} + o(1)$$

for some absolute constant c. Then one expects

$$\#\{\text{prime } p < X : a_p = 0\} \approx \sum_{p<X} \frac{1}{\sqrt{p}} = X^{1/2+o(1)},$$

where the last equality has used the Prime number theorem. This explains why our density should be 0: the number of primes less than or equal to X is $X/\log X$. However, it also tells us to expect there to be infinitely many primes p with $a_p = 0$.

Theorem 8 (Elkies)**.** Fix a non-CM elliptic curve $y^2 = f(x)$. Then there are infinitely many primes p such that $a_p = 0$.

Elkies achieves $\log\log X$ with $p < X$, which is of course far from expected.

As another example problem, we might have two non-CM elliptic curves $E_1 \colon y^2 = f_1(x)$ and $E_2 \colon y^2 = f_2(x)$, one might be interested in when $a_p(E_1) = a_p(E_2)$, where the a_p coefficients depend on E_1 and E_2. Well, one can imagine fixing $a_p(E_1)$, and as long as $a_p(E_1)$ is not too close in absolute value of $2\sqrt{p}$. So we expect the probability of $a_p(E_1) = a_p(E_2)$ to still be

Remark 9. It turns out that having $a_p(E_1) = a_p(E_2)$ always implies that we have an isogeny $E_1 \to E_2$ over $\overline{\mathbb{F}_p}$. (In fact, one can show that we only need to pass to an extension of $\mathbb{F}_p$ of degree with uniform bound based on the elliptic curve.) Basically, one shows that the eigenvalues of the aforementioned operator are off only by roots of unity.

1.2 Genus-2 Curves

Our genus 2-curves will look like $C \colon y^2 = f(x)$ where f has degree 5 and again has nonzero discriminant.

Example 10. Work with $C \colon y^2 = -x^6 - 4x^5 + 3x^4 + 2x^2 - 7x^2 - 62x + 42$. This turns out to be associated to the weight-2 cusp form

$$f(z) = q + aq^2 + (1-a)q^3 + q^4 - q^5 + (a-3)q^6$$

where $a = \sqrt{3}$. Here, the definition of $a_p \in \mathbb{Q}(\sqrt{3})$ is technical, but it turns out that $a_p \in \mathbb{Q}$ if and only if $C \pmod p$ admits a non-constant map to some elliptic curve over $\mathbb{F}_p$. Here are the first few values of a_p.

p	2	3	5	7	11	13	$\cdots$
a_p	$\sqrt{3}$	$1-\sqrt{3}$	-1	2	$\sqrt{3}-3$	1	$\cdots$

One can ask essentially the same questions about these coefficients $a_p(C)$. For example, it is known that $a_p(C) = 0$ has density 0, and we know that there are infinitely many primes p such that $C \pmod p$ has a non-constant map to some elliptic curve over $\overline{\mathbb{F}_p}$ (and the degree over $\mathbb{F}_p$ is bounded).

Remark 11. One can tell a similar story for higher-dimensional abelian varieties, as well as for function fields.

1.3 Infinitely Many Primes

As an application of what's going on here, we provide a proof that there are infinitely many primes.

Theorem 12. There are infinitely many primes.

Proof. Suppose for contradiction there are finitely many primes $p_1, \dots, p_r$.[1] We now bound $n!$. Now, prime-factor

$$n! = p_1^{\nu_1} \cdots p_r^{\nu_r}.$$

On one hand, we can upper-bound

$$\nu_i = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p_i^k} \right\rfloor \le \sum_{k=1}^{\infty} \frac{n}{p_i^k} = \frac{n}{p_i - 1} \le n,$$

so $n! \le (p_1 \cdots p_r)^n$. However, $n! \gg (n/2)^{n/2}$ because the product has $n/2$ terms at least $n/2$, so this bound is not possible. ∎

This sort of density argument is used frequently in arithmetic geometry: one often has access to bounds on some global object $n!$, so you decompose it into local intersections (here, prime factorization) and then compute to get bounds on the other side.

2 Hilbert's 10th Problem — Florian Sprung

In 1900, Hilbert posed 23 problems for mathematics, the motto being "We must know. We will know."

2.1 The 10th Problem

However, in his 10th problem, Hilbert asked to find an algorithm to determine whether a polynomial with integer coefficients has solutions in the integers. Of course, Hilbert had no rigorous notion of an algorithm or solution, but today we do.

However, it turns out that "we cannot know." Namely, it turns out that there is no algorithm to take a polynomial $P \in \mathbb{Z}[x_1, \dots, x_m]$ and determines whether there is a solution; this is due to Matiyasavič, building on work of many others. Hilbert was motivated by the fact that sometimes, for specific families of polynomials, there are solutions.

[1] One can make this proof effectively tell you the number of primes below some bound, but we will not.

Example 13. There is an algorithm which determines if $x^2 + y^2 = n$ has solutions. Here are some examples.

- $x^2 + y^2 = 2$ has solutions.
- $x^2 + y^2 = 3$ has no solutions.
- $x^2 + y^2 = 4$ has solutions.
- $x^2 + y^2 = 5$ has solutions.
- $x^2 + y^2 = 6$ has no solutions.
- $x^2 + y^2 = 7$ has no solutions.
- $x^2 + y^2 = 8$ has solutions.

In general, if n is prime, $x^2 + y^2 = n$ has solutions if and only if $n = 2$ or $n \equiv 1 \pmod 4$. One can stitch together the prime case into the general case: in general, $x^2 + y^2 = n$ has solutions if and only if $\nu_p(n)$ is even for all primes $p \equiv 3 \pmod 4$.

Remark 14. More generally, there is an algorithm to solve quadratic equations in two variables, namely of the form $ax^2 + bxy + cy^2 = n$. Roughly speaking, this boils down to the quadratic reciprocity law.

2.2 Diophantine Sets

The first idea here is to reverse the problem a little: instead of trying to take polynomials and finding solutions, we look at the sets cut out by Diophantine equations.

Example 15. The set $\{n : n = x^2 + y^2 \text{ for some } x, y \in \mathbb{Z}\}$ is a Diophantine set.

Definition 16 (Diophantine)**.** A subset $S \subseteq \mathbb{Z}$ is *Diophantine* if and only if there exists a polynomial $P \in \mathbb{Z}[y, x_1, \ldots, x_r]$ such that

$$S = \{n \in \mathbb{Z} : P(n, x_1, \ldots, x_r) = 0 \text{ for some } x_1, \ldots, x_r \in \mathbb{Z}\}.$$

Here, P is called the Diophantine equation associated to S.

Example 17. Any finite set is Diophantine: for a finite set S, define the polynomial

$$P(n) \coloneqq \prod_{s \in S} (n - s).$$

2.3 Computable and Listable Sets

The second idea was to introduce computable and listable sets. The intuition here is that computable sets are the best, and listable sets are second-best.

Definition 18 (computable)**.** A subset $S \subseteq \mathbb{Z}$ is *computable* if and only if there is an algorithm which takes in an integer $n \in \mathbb{Z}$ and determines if $n \in S$.

Definition 19 (listable)**.** A subset $S \subseteq \mathbb{Z}$ is *listable* if and only if there is an algorithm which takes in an integer $n \in \mathbb{Z}$ and outputs "yes" if $n \in S$ or outputs "no" or fails to halt if $n \notin S$.

We will continue to not be very rigorous about the notion of computability or algorithms; intuitively (by the Church–Turing thesis), it is enough to say that there is a Python program witnessing the algorithm.

Remark 20. Intuitively, this is called "listable" because one could imagine running the program Φ on all inputs in rough parallel and then listing out elements of S as the program Φ terminates on our parallel inputs. (Technically, we should run $\Phi(1)$ for 1 step, then run $\Phi(1)$ and $\Phi(2)$ for two steps each, then run $\Phi(1)$ and $\Phi(2)$ and $\Phi(3)$ for three steps each, and so on.) In this way, we can build a program which essentially (very slowly) outputs all elements of S.

Example 21. The set $\{n : n = x^2 + y^2 \text{ for some } x, y \in \mathbb{Z}\}$ is computable: for given n, test values of $x, y \in [-n, n] \cap \mathbb{Z}$ for solutions.

Example 22. Any Diophantine set is listable. Indeed, given a polynomial $P(y, x_1, \ldots, x_r)$, the computer program takes in $n \in \mathbb{Z}$ and tries out tuples $(x_1, \ldots, x_r) \in \mathbb{Z}^r$ waiting to see if $P(y, x_1, \ldots, x_r)$.

Quickly, we should remark the following.

Proposition 23. There are listable sets K which are not computable.

Proof. Roughly speaking, this is the Halting problem. Namely, find a computable way to list out all computer programs (for example, use hexadecimal representation of Python programs or something), and call the nth computer program Φ_n. Then define the set K defined by $n \in K$ if and only if Φ_n is a computer program which halts when given no inputs. The set K being computable would be equivalent to solving the Halting problem. ■

2.4 Diophantine Sets are Listable

Davis conjectured the converse of Example 22.

Conjecture 24 (Davis)**.** Any listable set is Diophantine.

Conjecture 24 would finish Hilbert's 10th problem. Indeed, find the polynomial $P_K(y, x_1, \ldots, x_r)$ corresponding to the listable (but not computable) set found in Proposition 23. Then having an algorithm to solve Diophantine equations would imply that we have an algorithm to determine if $P_K(n, x_1, \ldots, x_r) = 0$ has a solution when given $n \in \mathbb{Z}$, which is equivalent to having $n \in K$. But this violates K not being computable.

Davis was not able to prove Conjecture 24 alone. Robinson developed some techniques for Diophantine sets to attempt to get exponential growth. Then Davis, Putnam, and Robinson proved that if a single Diophantine equation had solutions sets growing exponentially, then listable sets would be Diophantine. Lastly, Matiyasavič managed to show that some linear recurrences were Diophantine, which finished the proof.

Theorem 25 (Davis, Putnam, Robinson, Matiyasevič)**.** Any listable set is Diophantine.

Remark 26. Here are some recent developments. Straightforward generalization works for $\mathbb{Z}[i]$, and the techniques work more generally for any abelian extensions. The question for more general rings of integers remains open, though there has been recent progress, using elliptic curves. Roughly speaking, if an elliptic curve of positive rank keeps its rank when moving to the larger field, then we get the result. For example, under BSD, one achieves

3 The Moduli Space of Elliptic Curves — Rose Lopez

A moduli space $\mathcal{M}$ is, roughly speaking, a parameter space where each point $p \in \mathcal{M}$ should correspond to some desirable object we are classifying. Today, we are interested in the moduli space $\mathcal{M}$ of all elliptic curves.

Remark 27. Roughly speaking, it turns out that the j-invariant of an elliptic curve characterizes the elliptic curve, so our moduli space is given by these j-invariants.

In general, for these moduli problems, we usually work over a fixed base scheme B; today we will (concretely) over the base schemes $\operatorname{Spec} k$ for a field k, to keep things simple. The problem now is to try to represent the functor $F\colon \mathrm{Sch} \to \mathrm{Set}$ taking the base scheme B to isomorphism classes of desirable B-schemes. In other words, we want a scheme M such that

$$FB \simeq \operatorname{Mor}_{\mathrm{Sch}}(B, M).$$

Concretely, when $B = \operatorname{Spec} k$ is a point, then we see want the k-points of M to correspond to isomorphism classes of desirable k-schemes. However, we have gained information about all base schemes B here. For example, we should imagine $\mathrm{id}_M \in \operatorname{Mor}(M, M) \cong FM$ as a space living over M, where fibers of particular k-points will correspond by base-change as needed. Also, objects with nontrivial automorphisms will become nontrivial automorphisms of M.

To continue, we pick up the following definition. Throughout, k is an algebraically closed field of characteristic not 2 or 3.

Definition 28 (elliptic curve)**.** An *elliptic curve* is a cubic of the form $E\colon y^2 = x^3 + ax + b$ such that $4a^3 + 27b^2 \neq 0$. The last condition essentially ensures that E is non-singular.

Definition 29 (j-invariant)**.** Given an elliptic curve $E\colon y^2 = x^3 + ax + b$, we define *$j$-invariant* as

$$j(E) \coloneqq \frac{1728a^3}{a^3 - 27b^2}.$$

One can check that the j-invariant does not depend on the isomorphism class of E; more precisely, an isomorphism is a structure-preserving bijection by

$$(x, y) \mapsto (\alpha y + \beta, \gamma x + \delta).$$

For example, we might have $\beta = 0$ and $\delta = 0$ and $\alpha^2 = \gamma^3$, so we have $(x, y) \mapsto \left(u^2 x, u^3 y\right)$ for some $u \in k$. Now, conversely, one can show that $j(E) = j(E')$ also implies an isomorphism $E \cong E'$.

Remark 30. In fact, for any $j(E) \in \mathbb{P}^1_{\mathbb{C}}$, one can find an elliptic curve with that j-invariant.

Remark 31. One can use these sorts of ideas to classify automorphisms of elliptic curves. For example, $a, b \neq 0$ has only two automorphisms coming from $u \in \{\pm 1\}$ as above; $a = 0$ automorphisms coming from u being a power of ζ_6; lastly, for $b = 0$, we have automorphisms coming from u being a power of i.

The above data tells us that our moduli space should be the affine line $\mathbb{A}_j$ with coordinate j; then $j = 0$ and $j = 1728$ are the elliptic curves with the above "extra" automorphisms. Technically, one should use a stack instead of a scheme here to keep track of these automorphisms.

4 Solving Transcendental Equations — Roy Zhao

Let's solve some equations and talk about what is it to do number theory.

4.1 Existential Closedness Problems

To start off, suppose we want to understand the system of equations

$$\begin{cases} a_1x_1 + a_2x_2 + a_3z_1 + a_4z_2 = a_5, \\ b_1x_1 + b_2x_2 + b_3z_1 + b_4z_2 = b_5, \\ c_1x_1 + c_2x_2 + c_3z_1 + c_4z_2 = c_5, \\ d_1x_1d +_2 x_2 + d_3z_1 + d_4z_2 = d_5. \end{cases}$$

Linear algebra tells us that this system will have a unique solution unless there is some linear relation between these equations, which we can check for by computing the determinant.

To make the question more interesting, we might want to add in some exponents to all these equations.

Theorem 32 (Bezout)**.** The number of solutions to a system of n equations in n variables (counted appropriately) is the product of the degrees of each of the equations, unless there is some relation between these equations.

So polynomials we more or less understand. As such, let's study things which aren't polynomials, such as

$$\begin{cases} a_1x_1 + a_2x_2 + a_3z_1 + a_4z_2 = a_5, \\ b_1x_1 + b_2x_2 + b_3z_1 + b_4z_2 = b_5, \\ z_1 = e^{2\pi i x_1}, \\ z_2 = e^{2\pi i x_2}. \end{cases} \tag{4.1}$$

Heuristically, we might imagine the equation $z_1 = e^{2\pi i x_1}$ as being some infinite-degree polynomial, from which we might conjecture that there are infinitely many solutions. Indeed, something like this is a conjecture of Zilber.

Conjecture 33 (Zilber)**.** A variety $V \subseteq \mathbb{C}^2 \times \mathbb{C}^2$ of dimension 2 has infinite intersection with the graph of the exponential function $\exp(2\pi i z)$.

Here, the dimension is enforcing that we do not have "relations" between our equations. Conjecture 33 has only been proven in limited cases, for example when we can parameterize z_1 and z_2 in terms of x_1 and x_2, as in (4.1).

4.2 Special Points

Here is an example problem: if both x and $e^{2\pi i x}$ are both algebraic numbers, then we say that $e^{2\pi i x}$ is a *special value*; then one can show that all special values are roots of unity. We now call $(z_1, \dots, z_n)$ a *special point* if its coordinates are special values. With this in mind, we say that an equation is *special* if and only if it is of the form

$$z_1^{e_1} \cdots z_n^{e_n} = \xi,$$

where ξ is a root of unity. The point is that we get a Zariski-dense subset of solutions arising from roots of unity.

One can now combine these inputs into the following theorem.

Theorem 34 (Manin–Mumford)**.** If the equations $f_1, \dots, f_{n-1} \in \mathbb{C}[z_1, \dots, z_n]$ have no algebraic relations (and so cut out a curve), and there are infinitely many special points as solutions, then each of the f_i themselves are special.

Remark 35. It is a conjecture of Zilber–Pink that merely having infinitely many solutions which are also solutions to two special equations is enough to conclude that each of the f_i are special.

Remark 36. An example generalization of the work we've done here is to use the j-function (which is transcendental) instead of the exponential map. One needs to translate the algebraic relations of the form $\exp(x+1) = \exp(x)$ into the symmetry conditions

$$j\left(\frac{az+b}{cz+d}\right) = j(z) \qquad \text{for all} \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

The notions of existential closedness and special points all go through just fine. Many transcendental functions can have these questions, such as the uniformization map for Shimura varieties, the exponential map for abelian varieties, period maps, and so on.

Remark 37. Here are a few useful tools which have shown up in the proofs of the aforementioned results.

- The techniques of o-minimality in logic have been fairly useful in proving these sorts of results.
- Algebraic number theory (e.g., relating Galois groups of special points to height functions, via the Weil height machine) have similarly been useful.
- Algebraic geometry has been used to relate height functions to L-functions.

5 Artin's Conjecture — Javier López-Contreras

Here is the question.

Conjecture 38 (Artin)**.** For any integer a which is not in $\{-1, 0, 1\}$ and is not a square, then $a \pmod p$ is a primitive root for infinitely many primes p.

Today we're going to introduce the conjecture.

Remark 39. Artin was able to conjecture a density result, estimating the number of such primes; Lehmer observed that the conjectured density was a little incorrect, but it was promptly corrected. Herbert Bilharz solved the corresponding problem in $\mathbb{F}_q[x]$. Hooley proved the result under GRH. The current progress, due to Heath-Brown, is that one of $\{2, 3, 5\}$ satisfies Artin's conjecture.

More precisely, Conjecture 38 is that the density of primes p such that $a \pmod p$ is a primitive root is

$$A(a) = \delta(a) \prod_p \left(1 - \frac{1}{p(p-1)}\right),$$

where $\delta(a)$ is a correction factor which is 1 most of the time. Let's explain this density. One can show that $a \pmod p$ is a primitive root if and only if each $\ell \mid p-1$ has $a^{(p-1)/\ell} \not\equiv 1 \pmod p$. As such, $a \pmod p$ will be a primitive root if and only if p is complete split in all the extensions $\mathbb{Q}(\zeta_\ell, a^{1/\ell})$, from which one can then use the Chebotarev density theorem. As such, one can show that the density of primes p with no $\ell \mid k$ for a fixed k is given by

$$A_k(a) = \sum_{d \mid k} \frac{\mu(d)}{\left[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}\right]}.$$

The nontrivial part of the conjecture is passing the limit to $k \to \infty$. Notably, one can compute the degree of the extension $\left[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}\right]$ as being $k\varphi(k)$ most of the time, and then write down the above infinite sum as an Euler product.

Remark 40 (Hooley)**.** Achieving GRH for the number fields $\mathbb{Q}\left(\zeta_k, a^{1/k}\right)$ will grant Artin's conjecture. Roughly speaking, one sieves the primes by intervals (it turns out that if $a \pmod p$ fails to be a primitive root, it will probably have witnesses ℓ roughly the size of $\log p$), reduces the problems to counting prime ideals with bounded norms, and then applying a prime-counting result with GRH input.

6 Bernoulli Numbers — Ellen Eischen

Today we're talking about four seemingly unrelated problems.

1. In general, we might be interested in computing the sums of powers
$$1^k + 2^k + \cdots + n^k$$
for positive integers n and k. For example, to sum $1+2+\cdots+n$, we first imagine doubling it by adding to it $n+(n-1)+\cdots+1$. In total, there are n pairs of $(n+1)$, so after dividing by 2, we have $n(n+1)/2$. However, this
2. We might be interested in the infinite series
$$\zeta(2k) \coloneqq \frac{1}{1^{2k}} + \frac{1}{2^{2k}} + \cdots.$$
3. We might be interested in solutions to $a^k + b^k = c^k$ in the positive integers.
4. The ring $\mathbb{Z}$ has unique prime factorization, so it is an interesting question to ask how this result might generalize to $\mathbb{Z}[\zeta_p]$, where ζ_p is a primitive pth root of unity.

6.1 Sums of Powers

Let's discuss the first question. Here are some cases for small k.

- One has $1^0 + 2^0 + \cdots + n^0 = n = \frac{1}{1}n^1$.
- One has $1^1 + 2^1 + \cdots + n^1 = n(n+1)/2 = \frac{1}{2}\left(n^2+n\right)$.
- By induction, one could show that $1^2 + 2^2 + \cdots + n^2 = \frac{1}{3}\left(n^3 + \frac{3}{2}n^2 + \frac{1}{2}n\right)$.

In general, one has the following.

Theorem 41 (Faulhaber)**.** For any positive integers n and k, one has
$$1^{k-1} + 2^{k-1} + \cdots + n^{k-1} = \frac{1}{k}\left(n^k + \binom{k}{1}B_1 n^{k-1} + \cdots + \binom{k}{k-1}B_{k-1}n^1\right)$$
where B_k is the kth Bernoulli number.

Proof. For fixed k, induct on n. Then induct on k. ∎

Remark 42. Intuitively, one could imagine defining $B^k = B_k$ as the kth Bernoulli number and then write
$$1^{k-1} + 2^{k-1} + \cdots + n^{k-1} = \frac{(n+B)^k - B^k}{k},$$
where the expression in the numerator is made sense of using the binomial theorem.

In fact, one can use the above theorem to define Bernoulli numbers recursively. Rigorously, we recursively define $B_0 = 1$ and $(B-1)^k = B_k$.

Example 43. We have $B_0 = 1$. We can solve for B_1 by noting $(B-1)^2 = B_2$, which gives $-2B_1 + 1 = 0$, so $B_1 = 1/2$. Then we can get B_2 by writing

$$B_3 = (B-1)^3 = B_3 - 3B_2 + 3B_1 - 1,$$

so we get $B_3 = \frac{1}{2}(3B_1 - 1) = \frac{1}{6}$.

Now, taking the above as a definition of our Bernoulli numbers, we can compute

$$(n+B)^k - (n + (B-1))^k$$

and then do an induction to get Theorem 41.

Here is a different definition of Bernoulli numbers.

Definition 44 (Bernoulli)**.** We define the Bernoulli numbers $\{B_k\}_{k=2}^{\infty}$ as

$$\frac{te^t}{e^t - 1} = 1 + \frac{t}{2} + \sum_{k=2}^{\infty} \frac{B_k}{k!} t^k,$$

where we have expanded as a Taylor series.

One can show that the definitions coincide by some kind of induction; namely, one can turn the generating function into a recursion, which matches up as needed.

6.2 Sums of Powers of Reciprocals

Euler showed that

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}, \qquad \dots.$$

More generally, we have the following.

Theorem 45 (Euler)**.** For any positive integer k, we have

$$\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = (-1)^{k+1} (2\pi)^{2k} \frac{B_{2k}}{2(2k)!}.$$

Proof. Omitted. There is a proof by the Herglotz trick to show

$$\pi \cot \pi x = \lim_{N \to \infty} \sum_{n=-N}^{N} \frac{1}{x+n}$$

and then expand out a Taylor series in both sides. ∎

Remark 46. This shows that the Bernoulli numbers have

$$|B_{2k}| = \left| \frac{\zeta(2k)}{(-1)^{k+1}(2\pi)^{2k}} \cdot 2(2k)! \right| \geq \left| \frac{2(2k)!}{(2\pi)^{2k}} \right|.$$

In particular, $|B_{2k}| \to \infty$ as $k \to \infty$ because the factorial is large.

6.3 Fermat's Last Theorem

The following is a hard result.

Theorem 47 (Wiles)**.** For $n \geq 3$, there are no positive integer solutions to the equation $a^n + b^n = c^n$.

Kummer had an approach to this problem as follows: it suffices to deal with the case where n is an odd prime and $n = 4$. Fermat had dealt with $n = 4$, so it remains to deal with the case where n is an odd prime. For this, we work in $\mathbb{Z}[\zeta_p]$, where we can factor

$$c^p = a^p + b^p = (a+b)(a+\zeta_p b)\left(a+\zeta_p^2 b\right)\cdots\left(a+\zeta_p^{p-1} b\right).$$

One can assume that $\gcd(a,b) = 1$, and then make some kind of nth power argument to conclude that $a+\zeta_p b$ should be a pth power under the assumption that $\mathbb{Z}[\zeta_p]$ has unique prime factorization. This holds for $p < 23$ but fails later.

In fact, Kummer discovered that he could get away with $p \nmid \#\operatorname{Cl}\mathbb{Q}(\zeta_p)$—namely, Kummer did not require the full power of being a unique factorization domain. Here, where $\operatorname{Cl}\mathbb{Q}(\zeta_p)$ is the class group of K. This grants us our definition.

Definition 48 (regular)**.** An odd prime p is *regular* if and only if $p \nmid \#\operatorname{Cl}\mathbb{Q}(\zeta_p)$.

We don't know if there are infinitely regular primes. It is true that $\#\operatorname{Cl}\mathbb{Q}(\zeta_p) \to \infty$ as $p \to \infty$. To see the Bernoulli numbers, we note that Kummer was able to check primes for regularity as follows.

Theorem 49. An odd prime p is *regular* if and only if p does not divide the numerators of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$.

Thus, we are motivated to understand how Bernoulli numbers behave under modulus. For example, for an odd prime p and nonnegative integer d, Kummer showed that $k \equiv \ell \pmod{\varphi(p^{d+1})}$ grants

$$\left(1-p^{k-1}\right)\frac{B_k}{k} \equiv \left(1-p^{\ell-1}\right)\frac{B_\ell}{\ell} \pmod{p^{d+1}}. \tag{6.1}$$

Notably, $\nu_p(B_k/k) \geq 0$ so that B_k/k makes sense in $\mathbb{Z}/p^{d+1}\mathbb{Z}$.

Remark 50. Roughly speaking, these ideas were continued by Iwasawa, whose theory played a central role in Theorem 47.

While we're here, we might as well discuss the p-adics for a little.

Definition 51. Given a rational number $\frac{a}{b}$, we define the p-adic absolute value as

$$\left|\frac{a}{b}\right|_p := p^{-(\nu_p(a)-\nu_p(b))},$$

where $\nu_p(n)$ refers to the largest power of p dividing n.

Example 52. One has $\left|\frac{3}{5}\right|_2 = 1$ because there are no powers of 2 here. One has $|100|_2 = \left|2^2\right|_2 = \frac{1}{4}$.

The point here is that we can read (6.1) as saying that $k \to \infty$ makes $\left(1-p^{k-1}\right)\frac{B_k}{k}$ converge. These sorts of ideas lead to p-adic interpolation and p-adic L-functions.

6.4 Kontsevich's Formula for Rational Plane Curves — Connor Halleck Dubé

Today we're doing enumerative algebraic geometry, so we are counting things associated to polynomial equations.

Example 53 (Apollonius)**.** Given three circles, how many circles are tangent to all three? The answer turns out to be eight: what's going on here is that such a circle is either inside or outside each triangle, so there are $2^3 = 8$ in total circles.

Today we want to count curves. For us, curves are going to projective curves in $\mathbb{P}^2_{\mathbb{C}}$. More precisely, $\mathbb{P}^2_{\mathbb{C}}$ is the moduli space of lines in $\mathbb{C}^2$, so points can be written down as $[x : y : z]$ where $(x, y, z) \neq (0, 0, 0)$, and $[x : y : z] = [\lambda x : \lambda y : \lambda z]$ for each $\lambda \in \mathbb{C}^\times$. For example, $\mathbb{P}^2_{\mathbb{C}}$ is a two-dimensional complex manifold or scheme or so on. To have a curve in projective space, we want to cut out by a single equation of the form

$$y^2 = x^3 - 1.$$

Technically, one should homogenize this to $y^2z = x^3 - z^3$ to cut a curve in $\mathbb{P}^2_{\mathbb{C}}$; this curve would have degree 3 because that is the degree of our homogeneous polynomial.

6.5 Counting Planar Curves

Here is an example question: how many curves of degree d are there through k (generic) points?

- For $(d, k) = (1, 2)$, we are asking for lines going through two (generic) points, for which is there is exactly one.
- For $(d, k) = (2, 2)$, we are asking for quadratics going through two points, for which there are infinitely many. (In fact, there is one dimension worth of these quadratics.)
- For $(d, k) = (1, 3)$, we are asking for lines going through

It turns out that $k = \frac{1}{2}\left(d^2 + 3d\right)$ is exactly the number of (generic) points needed to pin down one curve of degree d. More points, and we expect to have no curves; fewer points, and we expect to have infinitely many.

Remark 54. We take a moment to explicitly acknowledge that

We might want to measure our infinities. For this, we should discuss the moduli space of curves of fixed degree.

Example 55. Degree-3 plane curves are determined by 9 coefficients

$$a_0x^3 + a_1x^2y + a_2x^2z + a_3xy^2 + a_4xyz + a_5xz^2 + a_6y^3 + a_7y^2z + a_8yz^2 + a_9z^3 = 0.$$

However, scaling the coefficients does nothing, and we want to avoid the zero 9-tuple, so we see that our moduli space is actually $\mathbb{P}^8_{\mathbb{C}}$.

More generally, with degree d and three variables, we will have $\binom{d+2}{2}$ different coefficients. Expanding this out, we are setting $N \coloneqq \frac{1}{2}\left(d^2 + 3d\right)$ and looking in $\mathbb{P}^N_{\mathbb{C}}$.

Now, the condition of a curve containing a point we can see visually will turn into a linear condition on the coefficients of the polynomial. Thus, the moduli space of degree-d curves containing a fixed point p is a codimension-1 hyperplane in $\mathbb{P}^N_{\mathbb{C}}$. In total, N points in general position will impose N hyperplanes in $\mathbb{P}^N_{\mathbb{C}}$, which we see exactly will determine a point in $\mathbb{P}^N_{\mathbb{C}}$, which is what we wanted! The general position here is needed to ensure that these hyperplanes do not intersect unreasonably; one can check that this condition is Zariski open because we are basically asking to avoid some determinant vanishing.

6.6 Counting Rational Curves

Today, a curve $C \subseteq \mathbb{P}^2_{\mathbb{C}}$ is "rational" if and only if we can parameterize as $t \mapsto [x(t) : y(t) : 1]$. Equivalently, we can require a generically injective function $\mathbb{P}^1_{\mathbb{C}} \to C$.

Example 56. The curve $y^2z = x^3 - x^2z$ is rational by the map $t \mapsto \left[t^2+1 : t(t^2+1) : t\right]$. In contrast, curves of higher genus (such as elliptic curves) are

For our enumerative question, we want to know how many rational curves of degree d pass through k points. We could try to cut out the rational curves, but this is not so easy.

It turns out that we require $k = 3d-1$ points to pin down finitely many rational curves. For example, at $d = 1$, we are asking for the single line through a point. For degree 2, we need five points, which uniquely determine a curve of degree 2. But in degree 3, we are asking for 8 points in generic point, which will uniquely determine 12 curves.

So this problem is more interesting. Nonetheless, the approach is similar: build a moduli space of rational curves and examine the hypersurfaces cut out by requiring us to live in a particular point. To see how we build the moduli space, realize that we are more or less looking for images of degree-d maps $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$. One can parameterize these maps, but then one has to quotient by automorphisms of $\mathbb{P}^1_{\mathbb{C}}$, which then produces a stack as our moduli space. Anyway, this produces a moduli space M_d^{rat}.

We can now compute $\dim M_d^{\mathrm{rat}} = 3d-1$, which explains by some rough intersection theory why require $3d-1$ points to determine finitely many rational curves. However, M_d^{rat} is not compact, so one has to work a little harder to make it compact and then do the intersection theory in the compactification. Doing all this produces the following result.

Theorem 57 (Kontsevich)**.** Let N_d be the number of rational curves of degree d passing through $3d-1$ points in general position. Then there is a recurrence solving for N_d.

Remark 58. Kontsevich was actually a physicist, despite doing all this reasonably hard algebraic geometry. These problems came up organically!

The morals of the story are to use moduli spaces to understand families and to compactify your spaces.

6.7 An L-Function — Thomas Browning

Let's do something which isn't geometry. By way of example, we will work with the curve

$$C\colon x^3 + y^3 + z^3 = 0.$$

For example, the rational solutions $C(\mathbb{Q}) = \varnothing$ by Fermat's last theorem. Nonetheless, there are solutions over $\mathbb{F}_p$, which we can count: define $n_p \coloneqq \#C(\mathbb{F}_p)$. Approximately speaking, for any fixed x, we expect about p solutions based on what y and z should be, so we expect $n_p \approx p^2$. Let's see this.

Example 59. We can compute $n_2 = 4$ by placing a 0 in exactly one spot or everywhere. Here are some more numbers.

p	2	3	5	7	11	13	17	19	$\cdots$
n_p	4	9	25	55	121	109	289	487	$\cdots$

Notably, many of these look like squares.

In some sense, we are counting solutions incorrectly: after subtracting out by the solution $(0,0,0)$, we can multiply by any scalar in $\mathbb{F}_p^\times$ to produce sets of solutions. In this way, perhaps we should instead count

$$b_p \coloneqq \frac{n_p - 1}{p-1}.$$

Rigorously, this is the number of solutions in $\mathbb{P}^2_{\mathbb{F}_p}$. Here is our table.

p	2	3	5	7	11	13	17	19	$\cdots$
b_p	3	4	6	9	12	9	18	27	$\cdots$

Notably, the property that $n_p = p^2$ turns into $b_p = p+1$. As discussed before, we see $n_p \approx p^2$, so $b_p \approx p+1$. So we set $a_p \coloneqq (p+1) - b_p$, which is the following table.

p	2	3	5	7	11	13	17	19	$\cdots$
a_p	0	0	0	-1	0	5	0	-7	$\cdots$

So now we are interested in $a_p \approx 0$.

Remark 60. In fact, if $p \equiv 1 \pmod 3$, then $a_p = 0$. Indeed, in the original equation, $p \equiv 1 \pmod 3$ implies that the cubing map $x \mapsto x^3$ is a bijection, so C will have the same number of points as $x + y = z = 0$, for which there are indeed p^2 solutions.

Another pattern we might see is that $a_p \equiv -1 \pmod 3$ otherwise, which we won't sketch because it's harder. It is also true that $|a_p| \le 2\sqrt{p}$, which is a pretty sharp bound.

To build our L-function, we would like to extend a_p from primes to a sequence $\{a_n\}_{n\in\mathbb{N}}$.

Remark 61. One way to do this would be to define a_n by extending completely multiplicatively, but this turns out to be the incorrect definition, even though this will give us a good Euler product

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \left(\sum_{\nu=0}^{\infty} \frac{a_{p^\nu}}{p^{\nu s}} \right) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s}}.$$

Nonetheless, we might still want an Euler product of the form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \left(\sum_{\nu=0}^{\infty} \frac{a_{p^\nu}}{p^{\nu s}} \right),$$

so we will try to define a_n multiplicatively. It then remains to define a_n at prime powers. For example, it is not too behaved to try to count solutions in $\mathbb{Z}/p^k\mathbb{Z}$, but we could define

$$\widetilde{n}_{p^k} \coloneqq \#C\left(\mathbb{F}_{p^k}\right),$$

which have some nice properties. The corresponding $\widetilde{a}_{p^k} \coloneqq \left(\widetilde{n}_{p^k} - 1\right) / \left(p^k - 1\right)$. It is a surprising but true fact that these terms satisfy a recurrence $\widetilde{a}_{p^{k+1}} = a_p \widetilde{a}_{p^k} - p\widetilde{a}_{p^{k+1}}$, but this turns out to require $\widetilde{a}_1 = 2$.

Remark 62. One can explain this $\widetilde{a}_1 = 2$ because these point-counts have to do with traces of certain powers of operators, whence at 1 we are computing $1 + 1 = 2$.

The solution, now, is to ditch the point-counting but maintain the recurrence. Namely, we define $a_1 \coloneqq 1$ and $a_p \coloneqq \#C(\mathbb{F}_p)$ and then set

$$a_{p^{k+1}} = a_p a_{p^k} - p a_{p^{k-1}}.$$

Then we extend to all positive integers multiplicatively.

Remark 63. As motivation, one can show that

$$\exp\left(\sum_{k=1}^{\infty} \frac{\widetilde{a}_{p^k}}{k} T^k \right) = \sum_{k=0}^{\infty} a_{p^k} T^k$$

which turns out to be the correct definition.

In total, we have our L-function

$$L(s) \coloneqq \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \sum_{k=0}^{\infty} \frac{a_{p^k}}{p^{ks}} = \prod_{p \neq 3} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

It turns out that this L-function has all the correct properties, from meromorphic continuation to functional equation, and one can find some zero-free regions.

Remark 64. This L-function also arises from Hecke characters. Approximately speaking, one can show that $a_p \equiv 1 \pmod 3$ is the unique solution to $4p = a_p^2 + 27x^2$.

Remark 65. One also has

$$\sum_{n=1}^{\infty} a_n q^n = q \prod_{n=1}^{\infty} \left(1-q^{3n}\right)\left(1-q^{9n}\right)^2,$$

which is a modular form.

7 On the Origin of Modularity — Tony Feng

For our last talk, we will discuss modularity.

7.1 Motivation of Modularity

Let's warm up. A few times already, we've seen numbers which cannot be written as the sum of two squares. For example, not every number can be written as the sum of two squares: nothing $3 \pmod 4$ will suffice. Similarly, not every number can be written as the sum of three squares: nothing $7 \pmod 8$ will suffice. It turns out that we can write every number as the sum of four squares, due Lagrange.

Jacobi was able to achieve more: he could also count the number of ways to write a number as the sum of four squares.

Theorem 66 (Jacobi)**.** For any nonnegative integer n, let $r_4(n)$ be the number of ways to write n as the sum of four squares. Then

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d.$$

The idea in the proof is to define the q-series

$$\theta(z) \coloneqq \sum_{n=0}^{\infty} r_4(n) q^n,$$

where $q = e^{2\pi i z}$. It turns out that θ is a modular form, and assigning it a weight and level fits it into a two-dimensional modular form.

For θ functions in general, one fixes a lattice Λ equipped with a positive-definite quadratic form Q, and we define

$$\theta_Q(z) \coloneqq \sum_{n \geq 0} \#\{\lambda \in \Lambda : Q(\lambda) = n\} q^n.$$

For example, we recover the above θ with $\Lambda = \mathbb{Z}^4$ and $Q(a,b,c,d) = a^2+b^2+c^2+d^2$. As before, these functional equations inherit some extra symmetry conditions.

Remark 67. As more motivation, one can relate the Riemann ζ-function to a theta function θ, whereupon the symmetry condition on θ turns into the functional equation for ζ.

7.2 Geometric ϑ-functions

Proving that these θ functions are modular is based on the Fourier transform $\mathcal{F}$. The properties we will need today are that $\mathcal{F}$ Gaussians are self-dual and has the Poisson summation formula

$$\sum_{\lambda \in \Lambda} f(\lambda) = \sum_{\lambda^\vee \in \Lambda^\vee} \mathcal{F} f(\lambda^\vee)$$

for functions on $\Lambda \otimes \mathbb{R}$.

We might want to allow quadratic forms Q which are not positive-definite, but nonetheless, we do have a set $\mathbb{D}$ of maximal spaces of $\Lambda \otimes \mathbb{R}$ where Q is positive-definite, and one can provide it with a reasonable (hyperbolic) topology and so on. Then for each $W \in \mathbb{D}$, one has a counting problem Z_W, which is how we build the q-series.

Now, changing bases does not change the object, so we actually want to look at $\mathbb{D}/O(\Lambda)$. Further, the image $Z_W(n)$ for given n will trace out some geometric object $Z(n)$ in $\mathbb{D}$. It turns out that $Z(n)$ is a cycle on $\mathbb{D}/O(\Lambda)$, which lives in a suitable homology group. As before, taking a Fourier series produces a "ϑ cycle." It is a conjecture that

$$\vartheta(z) = \sum_{n \geq 0} Z(n) q^n$$

is a modular function, just valued in homology. However, everything is hard here, and little is known.

Remark 68. By way of analogy, θ is like cats and ϑ is like lions.

7.3 Positive Characteristic

So geometric ϑ functions are hard, but we hope that function-field analogues will be easier. Many of the constructions are similar, but we will avoid giving definitions rigorously because it requires some algebraic geometry to state precisely.

In positive characteristic, it turns out that the original θ functions are $r = 0$ as Θ_0. Then ϑ turns out to be $r = 1$ as Θ_1, and we can continue to a family in Θ_n. (There do not currently exist analogues in the number field setting, and we do not have the technology for it.) It is conjectured that all of these Θ_r have some suitable modularity.

Remark 69. Continuing the analogy, Θ_2 is like a saber-tooth tiger.

It is known that Θ_r is modular after deleting some positive codimension objects. Roughly speaking, we expect to be able to study all the Θ_r at once and see modularity in each from a more common structure.

To continue, we need some formalism. On a base field k, one has summation of and tensor product of k-vector spaces. For example, one can check that endomorphisms $T_1, T_2 \colon V \to V$ achieve

$$\operatorname{tr}(T_1 \oplus T_2) = \operatorname{tr} T_1 + \operatorname{tr} T_2 \qquad \text{and} \qquad \operatorname{tr}(T_1 \otimes T_2) = \operatorname{tr} T_1 \cdot \operatorname{tr} T_2.$$

Going further, one can talk about sheaves with direct sums and vector spaces, and we have much the same structure.

Example 70. The usual example of a sheaf is the set of continuous functions on a space S valued in a vector space V.

We even still have some notion of trace: a sheaf endomorphism $T \colon V \to V$ has a trace given by $x \mapsto \operatorname{tr} T(x)$, where $T(x)$ is the operator on the fiber $V(x)$.

Example 71. In order to Fourier analysis, we would like exponential functions. In sheaves, we want exponential objects among our sheaves. Roughly speaking, in sheaves, we want a sheaf $s \mapsto V(s)$ where we have

$$V(s_1 + s_2) = V(s_1) \otimes V(s_2)$$

for $s_1, s_2 \in S$. The point is that we are turning addition (roughly speaking) into multiplication. It's not obvious that such sheaves exist, but they do exist over (for example) $\mathbb{R}$ and $\mathbb{F}_p$.

With exponential sheaves, one can build the same sort of Fourier transform with self-dual integrality (i.e., a Poisson summation formula) and self-dual Gaussian sheaves. As such, we do achieve modularity of θ sheaves, suitably generalized. The same proof goes through.

Roughly speaking, we have produced a generalization for Θ_0, which we can recover from our modularity of sheaves as above by using the trace to produce the original Θ_0. To continue, we need some background. Recall that a short exact sequence

$$0 \to A \to B \to C \to 0$$

of (say) abelian groups will produce a long exact sequence

$$0 \to \mathrm{Hom}(D, A) \to \mathrm{Hom}(D, B) \to \mathrm{Hom}(D, C) \to \mathrm{Ext}^1(D, A) \to \mathrm{Ext}^1(D, B) \to \mathrm{Ext}^1(D, C) \to \cdots.$$

Approximately speaking, we can thus think of $\mathrm{Ext}^1(D, A)$ as the obstruction to exactness on the right. The point of introducing all of this is that we can upgrade endomorphisms $T \colon V \to V$ to endomorphisms actually living in $\mathrm{Ext}^r(V, V)$ for $r \geq 0$; applying the trace here does produce a cycle, which looks promising for our modularity! And indeed, we have the following.

> **Theorem 72.** For a "θ-sheaf" $\mathcal{S}$, one can find an endomorphism $\mathcal{S} \to \mathcal{S}$ and "derived" endomorphisms in $\mathrm{Ext}(\mathcal{S}, \mathcal{S})$ which produces Θ_r after taking the trace.

The point is that taking the trace now produces modularity in Θ_r for $r \geq 0$, up to the previously mentioned positive codimension pieces.