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 $a_p := N(p) - p$, 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 $a_p := p - N(p)$ 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 $|a_p| \leq 2\sqrt{p}$. 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 $-2 \leq a < b \leq 2$, 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 $p_1, \ldots, p_r$.[1] We now bound $n!$. Now, prime-factor

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

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

On one hand, we can upper-bound

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

so $n! \leq (p_1 \cdots p_r)^n$. 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 $P \in \mathbb{Z}[x_1, \ldots, x_m]$ 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.

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

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

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

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

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 $\mathrm{id}_M \in \mathrm{Mor}(M, M) \cong FM$ 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

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

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

$$\begin{cases} a_1 x_1 + a_2 x_2 + a_3 z_1 + a_4 z_2 = a_5, \\ b_1 x_1 + b_2 x_2 + b_3 z_1 + b_4 z_2 = b_5, \\ c_1 x_1 + c_2 x_2 + c_3 z_1 + c_4 z_2 = c_5, \\ d_1 x_1 d +_2 x_2 + d_3 z_1 + d_4 z_2 = d_5. \end{cases}$$

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

$$\begin{cases} a_1 x_1 + a_2 x_2 + a_3 z_1 + a_4 z_2 = a_5, \\ b_1 x_1 + b_2 x_2 + b_3 z_1 + b_4 z_2 = b_5, \\ z_1 = e^{2\pi i x_1}, \\ z_2 = e^{2\pi i x_2}. \end{cases} \tag{4.1}$$

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 $\exp(2\pi iz)$.

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 $e^{2\pi ix}$ are both algebraic numbers, then we say that $e^{2\pi ix}$ is a *special value*; then one can show that all special values are roots of unity. We now call $(z_1, \ldots, z_n)$ 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 $f_1, \ldots, f_{n-1} \in \mathbb{C}[z_1, \ldots, z_n]$ 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

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

The nontrivial part of the conjecture is passing the limit to $k \to \infty$. Notably, one can compute the degree of the extension $[\mathbb{Q}(\zeta_d, a^{1/d}) : \mathbb{Q}]$ 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.