Topics in Number Theory

taught by Manjul Bhargava and Jerry Wang

February 5, 2016

Introduction

Notes from Manjul Bhargava and Jerry Wang's class "Topics in Number Theory" at Princeton in Spring 2016.

Chapter 1

Overview

We'll talk about statistics for the number of rational points on curves, usually algebraic curves over $\mathbb{Q}$. (Later on we may change to another global field.)

The main question is the following:

- Given a "family" of algebraic curves over $\mathbb{Q}$ (ordered in some way), what "proportion" of those curves have a rational point? How many rational points do we expect on those curves?

The families will usually be given in terms of explicit equations with varying coefficients in $\mathbb{Z}$, giving these curves in projective space $\mathbb{P}^n$.

We'll order these curves by the maximum of absolute values of coefficients in $\mathbb{Z}$, called the **height** of the equation(s)/curve. (If it's a weighted projective space, then we have to take those weights into account.) We'll abuse langauge and refer to the equations as the curve (they're actually a model of the curve).

- When the curves in a family are ordered by height, what is the distribution of the number of rational points?

There are three types of behavior for rational points on curve.

Trichotomy:

1 Genus 0

Genus 0: A genus 0 curve over $\mathbb{Q}$ has either no rational points or its rational points are in bijection with $\mathbb{P}^1(\mathbb{Q})$. The key principle that makes it easier is that the **local-global principle** holds. A genus zero curve has rational iff it has $\mathbb{Q}_p$ poitns for all p and $\mathbb{R}$-points. Checking for $\mathbb{Q}_p, \mathbb{R}$ points is much easier. We just have to understand which curves locally have points everywhere; those curves globally have points.

Example 1.1.1 (Circles)**:** Consider $C_n : x^2 + y^2 = nz^2$ in $\mathbb{P}^2$. C_n has a rational point iff n is a sum of 2 squares iff the factorization of n has only even exponents for primes $\equiv 3 \pmod 4$.

The natural density of such n is 0. The average number of prime factors is infinite. The chance that none of the odd exponent primes are $\equiv 3 \pmod 4$ goes to 0.

This is not a good way of producing rational points.

We're not asking the right question. How 0 is 0—i.e. how fast is it approaching 0? The more precise answer is

$$|\{n < X : n \text{ is sum of 2 squares}\}| \sim \frac{cX}{\sqrt{\ln X}}.$$

This says how fast the density approaches 0.

It's easy to get unsolved problems, for example, if we allow arbitrary coefficients in front of x.

Example 1.1.2 (Diagonal conics)**:** Consider diagonal conics $C_{a,b,c} : ax^2 + by^2 + cz^2 = 0$ in $\mathbb{P}^2$. The density of $C_{a,b,c}$ having a rational point is 0. Asymptotics are different depending on your family.

Proof. We handle genus 0 curves with the local-global principle. By Chinese remainder theorem we can multiply a finite number of primes. To prove the proportion is 0, it suffices to show that when we take more and more primes, the density goes to 0. We're not using any infinite version of the CRT.

Take $p > 2$. How can we tell if it has a point over $\mathbb{F}_p$? A smooth conic always has a rational point. If How do we tell if the conic is smooth? Look at the determinant, it's smooth iff it's nonzero. The determinant is abc. If it's smooth it has a point over $\mathbb{F}_p$, by Hensel's lemma it lifts to a $\mathbb{Z}_p$ point.

The only way it has no points is if it's not smooth. If the conic is not smooth, it breaks up into 2 points. If the 2 lines are over $\mathbb{F}_p$, it still has smooth points, which lift to $\mathbb{Q}_p$ points. The only way it can not have points is if it is a product of two lines not defined over $\mathbb{F}_p$. There are no $\mathbb{F}_p$-points so no $\mathbb{Q}_p$-points.

- The probability that the determinant is a multiple of p ($p \mid abc$) is $1 - (1 - \frac{1}{p})^3 \approx \frac{3}{p} + O(p^2)$.
- Then the probability that the singular conic breaks up into two $\mathbb{F}_p$-conjugate lines over $\mathbb{F}_p$, i.e., the 2 lines are not defined over $\mathbb{F}_p$, is $\frac{1}{2}$. For example, if c is a multiple of p, we get $ax^2 + by^2 = 0$. The probability this doesn't factor is $\approx \frac{1}{2}$, the probability $\frac{b}{a}$ is not a square.

The density of $C_{a,b,c}$ having a point over $\mathbb{Q}_p$ is hence

$$\approx 1 - \underbrace{\frac{3}{p}}_{\mathbb{P}(p|abc)} \cdot \frac{1}{2} + O\left(\frac{1}{p^2}\right).$$

The density of cubics hving a $\mathbb{Q}_p$-point for all $p < Y$ is

$$\prod_{p<Y} \left(1 - \frac{3}{2p} + O\left(\frac{1}{p^2}\right)\right) \to 0.$$

As $Y \to \infty$ this goes to 0. □

(We did the calculations intuitively; it's worth going through this rigorously.)

(Alternatively we can try to fix a, b and let $c \to \infty$ for each a, b. This is what people have tried to do to understand the decay.)

What is the rate of decay to 0?

$$|\{|a|, |b|, |c| < X : C_{a,b,c} \text{ has a rational point}\} \ll \frac{X^3}{(\ln X)^{\frac{3}{2}}}.$$

The upper bound is due to Serre. He conjectured this should be a lower bound. This wasn't shown until later by Hooley (Representation of 0 by ternary quadratic forms). The analytic number theory gets technical, and he loses track of the constants quickly. Are the constants equal? Is it asymptotic with a fixed constant, or is it oscillating? This is unknown.

These are simple analytic number theory problems that we don't know the answer to.

The upper bound is straightforward with the right tool (large sieve). The lower bound is hard.

The real question for genus 0 curves is general conics.

Example 1.1.3 (General conic)**:** Consider

$$ax^2 + bxy + cxz + dy^2 + eyz + fz^2.$$

The density of such curves with a rational points is 0.

Proof. To get the rate of decay do the same proof. The probability that such a conic is singular over $\mathbb{F}_p$ is different. Take the determinant of the matrix $\begin{pmatrix} \frac{a}{2} & b & c \\ b & \frac{d}{2} & e \\ c & e & \frac{f}{2} \end{pmatrix}$. The determinant is equidistributed; the probability it's 0 is $\frac{1}{p}$. (This is different from the diagonal case. You can't just this by a diagonal conic.) Are they defined over $\mathbb{F}_p$? Again, it doesn't iff its singular and doesn't factor over $\mathbb{F}_p$, so the probability is $\frac{1}{2}$.

The probability that such a conic over $\mathbb{Z}$ has a $\mathbb{Q}_p$ point for all $p < Y$ is approximately

$$\prod_{p<Y} (1 - \frac{1}{2p}) \to 0$$

as $Y \to \infty$.

We expect

$$|\left\{a, b, c, d, e, f : \text{height} < X \text{ with } ax^2 + \cdots + fz^2 \text{ has a rational point}\right\}| \ll \frac{X^6}{\sqrt{X}}.$$

This was proved by Serre (it's what he really developed the large sieve for). It was open for 20 years what the lower bound is. Again it was done ($\gg \frac{X^6}{\sqrt{X}}$) by Hooley (Representation of zero by ternary quadratic forms II) in the last few years. Again, the precise asymptotics are unknown. □

The next frontier is finding the constant. Lower bounds are not a science yet; they tend to be ad hoc; there are common themes like the circle method. Upper bound sieves tend to be uniform.

The group action is implicit in Hooley's paper ("effecting linear changes of variable"). Hooley writes old-style. Perhaps if you translate it into modern group theory language it will be clearer.

Can you say anything about the height of the rational point (ex. to find it)? You have to use effective version of the local-global principle, which Cassel has bounds for. They're not very strong though.

There are many things in genus 0 we don't quite understand yet.

2 Genus 1

The main issue is that the local-global principle does not always hold. You need global arguments as well.

The famous example is

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

due to Selmer. This has points over $\mathbb{Q}_p$ for all p and over $\mathbb{R}$ but not over $\mathbb{Q}$. This has an another level of algebraic difficulty.

The first simplification is to suppose that our curve locally has points everywhere, so much so that it has a global point. Take a family of curves where you already have a rational global point; then there are no local obstructions to having points.

Example 1.2.1: Thus, the first natural case is a genus one curve coming with a marked rational point, i.e., an **elliptic curve**.

Any elliptic curve over $\mathbb{Q}$ can be expressed as $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$. We embedded the curve using the divisor $3(P)$ where P is the marked point, and then changed variable. The rational points of $E = E_{A,B}$ form an abelian group where the marked point is the identity, denoted $E(\mathbb{Q})$. (The group is the same as the divisor class group.)

Mordell showed that $E(\mathbb{Q})$ is finitely generated. Once you have a marked point, you have a group of rational points. It's abelian and finitely generated. We can ask about statistics of the group.

The discriminant is $-4a^3 - 27b^2$. In terms of modular forms these are the G_4, G_6 of the corresponding lattice; G_4^3, G_6^2 are comparable. It's natural to define the height

$$H(E_{A,B}) = \max\{|4A^3|, |27B^2|\}.$$

How are the groups distributed in the space of finitely generated abelian groups?

That it is finitely generated means

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$$

where r is the **rank** and T is finite (the torsion group). It turns out that $|T| < 16$ by Mazur. It's easy to show that 100% of the time $|T| = 1$. To get $|T| = c > 1$, certain algebraic things happen to a, b; they have to be on a subvariety. There are finitely many of these subvarieties, so there's probability 0 it's on one of them.

For $r = 0$ there are finitely many rational points. For $r \geq 1$ there are infinitely many. The rank quantifies how "infinitely many" you are.

The statistics of the number of rational points is not so interesting. We can distinguish them by the rank.

The natural questions are not about the number of rational points but about the distribution of the rank r. In particular, do they have finitely many points or infinitely many points more often? When they have infinitely many points, what does the rank tend to be?

Do elliptic curves tend to have finitely many or infinitely many rational points? People guessed both, and they were both wrong.

Goldfeld looked at families of twists of elliptic curves. Katz-Sarnak used a the big book of random matrix philosophy.

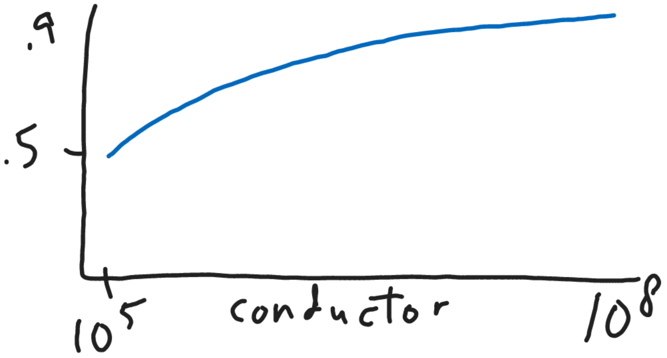
Conjecture 1.2.2 (Goldfeld, Katz-Sarnak)**:** The average rank of elliptic curves over $\mathbb{Q}$ is $\frac{1}{2}$. More precisely, 50% have rank 0 and 50% have rank 1.

There are infinite families of curves with rank 2, but they are very sparse. As long as you order by something not correlated with rank (ex. conductor, discriminant, height), we think it should be true (no formal equivalence is known though). The number of curves of conductor $< X$ should be $X^{\frac{5}{6}}$. A goes up to $X^{\frac{1}{3}}$ and B goes to $X^{\frac{1}{2}}$. We don't know this yet—it's something we need to answer first.

The best bounds are due to Duke, who shows a $o(X)$ upper bound. There are many ingredients. One has to use class group bounds, modularity, etc. You can get a lower bound of $X^{\frac{5}{6}}$.

If you solve this problem, presumably a lot of theorems we prove for height can be adapted to if we order by conductor.

Katz-Sarnak were busy writing their book. They had their manuscript floating around. People (Brumer-Mebuinness, Bektemerov-Stein-Watkins) were doing these computations of ranks. There was no correlation between what the computations were saying and what the conjecture was saying. We made a graph.



Moreover, the number of rank 2 curves went up to ≈ 20%. Katz-Sarnak though the graph would turn around. But they believed in their random matrix philosophy. That's what got me interested in the problem as a grad student.

At that time, one couldn't even prove that the average rank is greater than 0 or less than ∞. One of the goals I set out to do was to prove this.

What was known?

- Based off an idea of Goldfeld, Brumer and Heath-Brown gave the first theoretical evidence that the average rank is bounded. The average rank is going up; people on the data side weren't even sure the average rank is finite.

  If you assume BSD and GRH for L-functions of elliptic curves (2 million dollars of conjectures). Then the average rank is ≤ 2.3 (Brumer) and ≤ 2 (Heath-Brown).

  Heath-Brown tried to get < 2, because that would imply a positive proportion have rank 0 or 1.

- Young showed with the same assumptions that the average rank is ≤ 1.7.

Can we show this by leaving the analytic and L-function world and using algebraic techniques? Can we combine these two techniques?

Theorem 1.2.3 (Bhargava, Shankar)**:** The average rank is bounded and in fact is $< .885$.

We'll start talking about the proof of this next week and Shankar will finish it the fourth week. The final ideas involved root numbers.

Theorem 1.2.4 (Bhargava, Skinner, Wei Zhang)**:** The average rank is strictly positive, and in fact $> .2$.

This is tricky because you have to construct rational points. The point constructions are done using work of Skinner and Urban. The expected is 0.5—this looks good for the conjecture.

The graph goes past .9 now (after another order of magnitude), so it has to turn around! When A, B are small, it's easier for coincidences to happen. There's still around 20% of rank 2 curves, and it's still not going down. It looks like we'll have to compute quite a bit further.

The results are proved using 2-Selmer and 5-Selmer groups. If these methods continue to work for n-Selmer groups for higher n, then the bounds will approach 0.5. This gives another way to conjecture that the true average rank is 0.5.

Their conjectures work over other global fields; we get a universal bound < 1.05 over any global fields of characteristic $\neq 2$. The techniques indicate that the conjecture should be true over other global fields. More is not known for function fields. The lower bound does not work because we need to apply Gross-Zagier (totally real fields probably work). Jerry will talk about generalizing the bounds to any number field.

Corollary 1.2.5 (of proof)**:** A positive proportion ($> 20\%$) of elliptic curves over $\mathbb{Q}$ have rank 0.

Corollary 1.2.6 (of proof)**:** A positive proportion ($> 20\%$) of elliptic curves over $\mathbb{Q}$ have rank 1.

(Arul will explain how to get this with root numbers.)

Corollary 1.2.7 (together with work of Wei Zhang)**:** A positive proportion ($> 20\%$) of elliptic curves over $\mathbb{Q}$ have analytic rank 0, 1.

Theorem 1.2.8: A positive proportion ($> 66\%$) of elliptic curves satisfy the Birch and Swinnerton Dyer rank conjecture.

What if any obstacle is there to taking 5-Selmer to higher Selmer groups? We think it's a question of algebraic geometry. The algebraic geometry we used was classical stuff known in the 18th century. Presumably we can do better.

Example 1.2.9: A genus 1 curve with a degree 2 divisor, i.e., a degree 2 map to $\mathbb{P}^1$. (In Example 1.2.1 we had a degree 1 divisor.) By Riemann-Hurwitz, it has 4 ramification poitns, so such a curve can be expressed as

$$z^2 = f(x, y)$$

where f is a binary quartic form.

This is not an elliptic curve because it may not necessarily have rational points. We may get 2 points at ∞ that may be conjugate to one another. (The usual way you see this is $z^2 = f(x)$ where f is a quartic polynomial.)

We can ask the same question: varying the 5 coefficients, how are the rational points distributed?

All the theorem use each other!

Theorem 1.2.10: If all binary quartic forms $ax^4 + bx^3y + cx^2y^2 + dxy^3 + dxy^3 + ey^4$ $(a, b, c, d, e \in \mathbb{Z})$ are ordered by height,

1. A positive proportion ($> 75\%$) of $z^2 = f(x, y)$ have a point over $\mathbb{Q}_p$ for all p and over $\mathbb{R}$.

   This is very different from the genus 0 case. (We will show a sieve technique, for any genus 1 or higher curve, to get lower bounds.)

2. A positive proportion ($< 75\%$) of $z^2 = f(x, y)$ have a point everywhere locally but no point over $\mathbb{Q}_p$ (they fail Hasse).

3. A positive proportion of $z^2 = f(x, y)$ hve a rational point.

All 4 possibilites (local points everywhere? global points?) occur a positive proportion of the time.

Example 1.2.11: Genus 1 curves in $\mathbb{P}^2$ (corresponding to a genus 1 curve with a degree 3 divisor), i.e., a smooth plane cubic, i.e., a ternary cubic form, which has 10 coefficients:

$$ax^3 + bx^2y + \cdots + jz^3 = 0.$$

This is the most common cubic that people talk about: smooth cubics in the plane.

Theorem 1.2.12: The same theorem holds for genus 1 curves in $\mathbb{P}^2$.

Example 1.2.13: Genus 1 curves in $\mathbb{P}^3$ (corresponding to a genus 1 curve with a degree4 divisor), i.e., two quadrics in $\mathbb{P}^3$, i.e., two quaternary quadratic forms. They are given by 2 4×4 matrices with coefficiens $a, b, c, d, e, f, g, h, i, j; k, l, m, n, o, p, q, r, s, t,\ a, \dots, t \in \mathbb{Z}$ (20 coefficients).

This is a complete intersection: any genus 1curve in $\mathbb{P}^3$ can be represented this way, and conversely, given two quadrics, generically they will intersect in genus 1 curve. This is a full description of genus 1 curves in $\mathbb{P}^3$.

Theorem 1.2.14: The same theorem holds for genus 1 curves in $\mathbb{P}^3$.

These are all classical objects in 18th century algebraic geometry.

There's one more example.

Example 1.2.15 (Example 5)**:** Genus one curves in $\mathbb{P}^4$. This is NOT a complete intersection. Generically, 5 quadrics intersect in nothing. Many people gave up; some persisted. You can completely describe them as well.

This is a quintuple of 5×5 skew symmetric matrices A, B, C, D, E.

How to make a genus 1 curve using 5×5 skew symmetric matrices? Given A, B, C, D, E, you can make a single 5×5 matrix of linear forms

$$Ax + By + Cz + Dt + Eu.$$

We can takes its determinant? The determinant is 0 because it's an odd skew-symmetric matrix.

What if we take the determinant of a 4×4 skew-symmetric matrix? It's a square. It's a degree 4 form in 5 variables. Taking its square root we get a quadric. There are 5 primary (on-diagonal) 4×4 matrices.

The square root of the determinant is called the **Pfaffian**. The Pfaffian of any primary 4×4 block of $Ax + By + Cz + Dt + Eu$ gives a quadric in $\mathbb{P}^4$.

We get 5 quadrics $Q_1, \dots, Q_5$ in $\mathbb{P}^4$. Classical algebraic geometers noted that

$$Q_1 \cap \dots \cap Q_5$$

is a genus 1 curve in $\mathbb{P}^4$. Conversely any genus 1 curve embedded by a complete linear system is given uniquely (up to change in basis) as $Q_1 \cap \dots \cap Q_5$ where $Q_1, \dots, Q_5$ come from a unique (A, B, C, D, E), a quintuple of 5×5 skew-symmetric matrices.

These case $\mathbb{P}^1$ helps us understand 2-Selmer, up to $\mathbb{P}^4$ helping us understand 5-Selmer. This is the last case we know how to solve.

The problem in general is to describe how to use this to understand Selmer. The open question is how can we study genus 1 curves in higher projective spaces?

Index