LECTURE NOTES FOR
BHARGAVAOLOGY LEARNING SEMINAR
JANUARY TO APRIL 2015

STANLEY YAO XIAO

ABSTRACT. These are the course notes that I am lecturing out of for the learning seminar on 'Bhargavaology', which is the colloquial term used to describe the subjects of number theory strongly influenced or advanced by Manjul Bhargava.

CONTENTS

1. INTRODUCTION TO BHARGAVAOLOGY BY STANLEY XIAO

ABSTRACT. In this introductory talk I aim to give a sampling of the vast nest of important theorems related to Manjul Bhargava, one of the four Fields Medalists of 2014, and describe their importance in the context of modern number theory. There are no technical details in the talk, making it very accessible.

'Bhargavaology' is a colloquial term, coined by students and collaborators of Manjul Bhargava, to describe his immense contributions to the field of number theory. Roughly speaking, Bhargavaology can be sketched as the following: suppose we wish to count some family of arithmetic objects. Typically, objects in this family are characterized by some invariant. However, sorting these objects by this invariant, while natural, seems to be very hard. Instead, one constructs a 'naive' height which mimics the invariant(s) and sort by that instead. Then Bhargava and his collaborators have shown that if one does this, then one can usually obtain fantastic success when trying to count 'generic' objects in the family. Below is a sampling of theorems that have been achieved using Bhargava's methods:

Theorem 1.1. *(Bhargava, Shankar, Tsimerman 2013) Let $N_3(\xi, \eta)$ denote the number of cubic fields $K/\mathbb{Q}$, up to isomorphism, that satisfy $\xi < \operatorname{Disc}(K) < \eta$. Then*

$$N_3(0, X) = \frac{1}{12\zeta(3)}X + \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O_\epsilon\left(X^{5/6-1/48+\epsilon}\right);$$

$$N_3(-X, 0) = \frac{1}{4\zeta(3)}X + \frac{\sqrt{3}\cdot 4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O_\epsilon\left(X^{5/6-1/48+\epsilon}\right).$$

Theorem 1.2. *(Bhargava, 2014) A hyper elliptic curve C over $\mathbb{Q}$ has a model in $\mathbb{P}(1, 1, g+1)$ with the equation*

$$z^2 = f(x, y) = f_0x^{2g+2} + f_1x^{2g+1}y + \cdots + f_{2g+2}y^{2g+2},$$

where g is the genus of the curve C. Define the height $H(C)$ to be $\max\{|f_i|\}$. Let

$$\rho_g = \limsup_{X\to\infty} \frac{\#\{\textit{curves } C \textit{ with a rational point of height at most } X\}}{X}.$$

Then

$$\lim_{g\to\infty} \rho_g = 0.$$

Theorem 1.3. *(Bhargava, Skinner, Zhang 2014) For an elliptic curve $E/\mathbb{Q}$, it has a model of the form*

$$E : z^2 = x^3 + Ax + B, \ A, B \in \mathbb{Z}.$$

Define the height of E to be $\max\{4|A|^3, 27B^2\}$. Define

$$\rho = \limsup_{X\to\infty} \frac{\#\{\textit{elliptic curves } E/\mathbb{Q} \textit{ satisfying the Birch-Swinnerton-Dyer conjecture of height at most } X\}}{X}.$$

Then $\rho \geq 0.6648$.

Theorem 1.4. *(Bhargava, Shankar 2013)* [2] *Suppose $E/\mathbb{Q}$ is an elliptic curve. Then the set of rational points on E which we denote by $E(\mathbb{Q})$ forms an abelian group. Thus $E(\mathbb{Q}) \cong G \oplus \mathbb{Z}^r$,* *where G is a finite abelian group. The number r is called the* <u>*rank*</u> *of E, which we denote by* $\operatorname{rank}(E)$. *Define*

$$\operatorname{Avg}_X = \frac{1}{X} \sum_{H(E) \leq X} \operatorname{rank}(E)$$

and

$$\operatorname{Avg} \operatorname{rank} = \limsup_{X \to \infty} \operatorname{Avg}_X .$$

Then

$$\operatorname{Avg} \operatorname{rank} \leq 1.5.$$

Theorem 1.5. *(Bhargava, Shankar 2014) In fact, we have* $\operatorname{Avg} < 0.885$. *Further, there are at least* 83.75% *of elliptic curves over* $\mathbb{Q}$ *with rank* 0 *or* 1.

Theorem 1.6. *(Bhargava, Skinner 2014) There exists a positive proportion of elliptic curves over* $\mathbb{Q}$ *with rank at least 1.*

Theorem 1.7. *(Bhargava, Shankar 2012-2014) We have the following averages for Selmer groups:*

- $\operatorname{Avg} \operatorname{Sel}_2(E) = 3$,
- $\operatorname{Avg} \operatorname{Sel}_3(E) = 4$,
- $\operatorname{Avg} \operatorname{Sel}_5(E) = 6$.

To give an idea of the scope of these ideas, let us consider why some of these questions are hard. The first theorem is an improvement of the classical theorem of Davenport and Heilbronn, one of the crowning achievements of the theory of geometry of numbers. The difficulty here is that the interesting region does not grow homogeneously, which is usually a critical feature in problems involving geometry of numbers. Instead there exist bad ‘cusps’ that keep growing out of control as one scales the region, and Davenport showed how to ‘cut it off’ in his original arguments. The key insight of Bhargava, which is pervasive in nearly all of his works, is that while the cusp may have volume comparable to the main body, if suitably controlled the cusp only contains ‘bad’ objects (or non-generic objects), so may be ignored anyway if one only wants to count generic objects. The idea of ‘generic’ is loose; it varies from context to context.

The second theorem is related to the celebrated theorem of Faltings (which won him the Fields Medal in 1986), which asserts that any curve over $\mathbb{Q}$ with genus at least two has at most finitely many rational points, settling the conjecture of Mordell. However, Faltings’ theorem is notoriously <u>ineffective</u>. That is, we do not know of a way to bound the height of the rational points which may lie on curves, and so we never know if we found them all. Further, by the very general ‘minimalist’ conjecture, which asserts that unless there is a reason for an algebraic variety to have rational points, then there probably aren’t any points, one ought to expect that most curves of genus $g \geq 2$ has no rational points at all! However, this is very hard to prove; in fact just proving that the genus $\lfloor n/2 \rfloor$ curve

$$x^n + y^n = z^n$$

have no rational points is already supremely difficult, and that’s just one curve! This should illustrate the immensity of Bhargava’s theorem.

Perhaps another word is necessary for the difficulty of Bhargava’s theorem. The most natural way to try to prevent the existence of rational points is to try to obtain a local obstruction. That is, suppose we have a diophantine equation

$$f(x_1, \cdots, x_n) = 0$$

for some polynomial f defined over $\mathbb{Q}$. If this equation fails to have a solution mod p for some prime p or over the real numbers, then surely it cannot have rational points! For instance

$$x^2 + y^2 = -4$$

cannot have any rational points because it doesn't even have a real point. The curve

$$x^2 + y^2 = 3$$

cannot have any rational points because it fails to be solvable mod 4, since the sum of two squares is never congruent to $3 \pmod 4$. However, this novel approach fails because of the following (perhaps unfortunate) fact. We say that an algebraic variety V is everywhere locally soluble, or ELS, if it contains a point over $\mathbb{Q}_p$ for any prime p, and a point over $\mathbb{R}$.

Fact 1.8. *A proportion approaching* 100% *(as the genus g goes to infinity) of hyperelliptic curves are ELS!*

This means, in light of Bhargava's theorem, that nearly 100% of hyperelliptic curves have local points everywhere, but nevertheless fail to have a global point. This means it fails the local-to-global principle, otherwise known as the Hasse principle.

As an aside, Bhargava's theorem is a major breakthrough in the following conceptual deadlock: frequently one obtains an upper bound for the number of points of an algebraic curve defined over some field in terms of its genus. However, the bound typically grows with the genus, which is counterintuitive: we expect curves of higher genus to have less points than curves of lower genus. Bhargava's work might give us the 'correct' way to bound the number of rational points in general.

Returning to the so-called 'minimalist' conjecture, a specific manifestation of this is a conjecture of Katz and Sarnak

Conjecture 1.9. $\operatorname{Avg}\operatorname{rank} = 1/2$*, with exactly* 50% *of elliptic curves over* $\mathbb{Q}$ *having rank 0 and exactly* 50% *having rank 1.*

This is based on the following heuristic: half the time the rank should be even, and half the time it should be odd. When it's even it wants to be the smallest possible, so it ends up being 0. When it's odd it also wants to be as small as possible, so it ends up as 1. In this context, the bound of Bhargava-Shankar is very close to being optimal.

Perhaps another illustration of the power of Bhargavaology is the history of the average rank problem. Various mathematicians, including most recently D.R. Heath-Brown, have obtained upper bounds for $\operatorname{Avg}\operatorname{rank}$ assuming the Generalized Riemann Hypothesis. Nevertheless, the bound that Heath-Brown obtained was worse than the unconditional bound obtained by Bhargava and Shankar! When you can beat the GRH, then you must have landed on something good!

Next, let us discuss Bhargava's contribution in the context of the Birch-Swinnerton-Dyer conjecture, which we will refer to as BSD. For any elliptic curve $E/\mathbb{Q}$, we defined $\operatorname{rank}(E)$ as the number of copies r of $\mathbb{Z}$ that $E(\mathbb{Q})$ has in its abelian group decomposition. This is the natural definition of rank, and it is also called the algebraic rank. There is another way to define rank. For a given curve E, we may attach an L-function to it. Let $E(\mathbb{F}_p)$ denote the reduction of E modulo p, and define $a_p = p + 1 - \#E(\mathbb{F}_p)$. Then the L-function of E is

$$L(E, s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

This function may have a zero at $s = 1$, and since one can show that L is meromorphic, it follows that one can naturally find the order of that zero at $s = 1$. Then BSD asserts that this order, which we call the analytic rank of E, is equal to the algebraic rank.

We note that BSD is in fact one of the seven millennium problems, which in this context means it is comparable to the Riemann Hypothesis of the Poincare Conjecture. The fact that we know that a large percentage of elliptic curves over $\mathbb{Q}$ satisfy BSD is a tremendous milestone in mathematics. Previous to the work of Bhargava, Skinner, and Zhang, it wasn't even known if BSD is true for a single elliptic curve!

Over the next few months I wish to go over some of these results with you, and perhaps some of you might share your thoughts as well.

2. Binary quartic forms and average ranks of elliptic curves (1/3) by Stanley Xiao

ABSTRACT. In this talk I aim to describe the approach taken by Bhargava and Shankar to show that the average rank of elliptic curves is bounded. It turns out that the key observation is controlling the average size of various Selmer groups. Various improvements on the bound for the rank depends on knowledge of $2, 3, 5$-Selmer groups, respectively. In the 2-Selmer case, the key is to count 2-Selmer elements via a bijection with binary quartic forms, thus turning the problem of bounding the rank of elliptic curves into counting equivalence classes of integral binary quartic forms.

In the next few talks we aim to sketch the ideas found in [2], [3], and [4]. Combined these papers represent over 100 pages of mathematical material published or soon to be published in a top journal (Annals of Mathematics), so we obviously can't hope to learn all of the details in a few lectures. That said, I hope that the main ideas will become clear. We start with [2], where the main ideas should already become apparent.

Recall that an elliptic curve $E/\mathbb{Q}$ can be given by an equation of the form

$$y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Z}.$$

If we assume further that for all primes p such that $p^4 | A$ we have $p^6 \nmid B$, then this representation is unique. Recall that we defined the (naive) height of the elliptic curve $E = E_{A,B}$ as

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

The main connection between the size of the Selmer group and the rank of elliptic curves is the following exact sequence:

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E) \to Ш_E[2].$$

Here $\mathrm{Sel}_2(E)$ is the 2-Selmer group of E, and $Ш_E[2]$ is the 2-torison part of the Tate-Shafarevich group of E.

Recall that an exact sequence of groups $0 \to G_1 \to \cdots \to 0$ refers to a sequence of homomorphisms $\phi_j : G_j \to G_{j+1}$ such that $\mathrm{im}(\phi_j) = \ker(\phi_{j+1})$. If we write

$$E(\mathbb{Q}) = G \oplus \mathbb{Z}^r,$$

then

$$E(\mathbb{Q})/2E(\mathbb{Q}) = (G/2G) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z}).$$

Hence, we see that $2^r \leq \# \mathrm{Sel}_2(E)$, whence knowledge of the size of the Selmer group would give us information on the rank!

Now we need to understand how an accurate count of binary quartic forms gives information about elliptic curves or Selmer groups! The connection is an ingenious observation due to Birch and Swinnerton-Dyer in the 1960s. To state their observation, we must first introduce some terminology. First, we need to give an interpretation of the 2-Selmer group itself. It can be thought of as the set of “locally soluble 2-coverings" of an elliptic curve $E/\mathbb{Q}$. A 2-covering of $E/\mathbb{Q}$ is a genus one curve $C/\mathbb{Q}$ along with two maps $\phi : C \to E$ and $\theta : C \to E$ where ϕ is an isomorphism defined over $\mathbb{C}$ and θ is a degree 4 map such that we have the composition

$$\phi \circ [2] = \theta$$

where $[2]$ denotes the map that sends a point P on E to $2P$. Now, a soluble 2-covering is one which possesses a rational point, whereas a locally soluble 2-covering is one that possesses a $\mathbb{Q}_p$ point for every prime p and a point over $\mathbb{R}$. The following bijections are established

$$\{\text{soluble 2-coverings}\}/\sim \leftrightarrow E(\mathbb{Q})/2E(\mathbb{Q})$$
$$\{\text{locally soluble 2-coverings}\}/\sim \leftrightarrow \mathrm{Sel}_2(E).$$

Now, Birch and Swinnerton-Dyer showed that any locally soluble 2-covering c possesses a canonically associated degree 2 divisor defined over $\mathbb{Q}$, thus yielding a double cover $C \to \mathbb{P}^1$ ramified at 4 points. We thus obtain a binary quartic form over $\mathbb{Q}$, well defined up to $\mathrm{GL}_2(\mathbb{Q})$-equivalence! This connection between elements in the 2-Selmer group and binary quartic forms was first used by B-SD in their original elliptic curve computations, which lead to their famous conjecture. This approach remains one of the fastest practical ways of computing ranks of elliptic curves.

Now, let us state a few theorems in [2] which makes this connection precise.

Theorem 2.1. *(Theorem 3.2 in [2]) Let K be a field having characteristic not equal to 2 or 3. Let*

$$E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$$

be an elliptic curve over K. Then there exists a bijection between elements in $E(K)/2E(K)$ and $\mathrm{PGL}_2(K)$-orbits of K-soluble binary quartic forms having invariants I and J, given by

$$(\xi, \eta) + 2E(K) \mapsto \mathrm{PGL}_2(K) \cdot \left(\frac{1}{4}x^4 - \frac{3}{2}\xi x^2y^2 + 2\eta xy^3 + \left(\frac{I}{3} - \frac{3}{4}\xi^2\right)y^4\right).$$

(We will describe the invariants I and J shortly).

Theorem 2.2. *(Theorem 3.5 in [2]) Let $E = E^{I,J}$ be an elliptic curve over $\mathbb{Q}$ (with invariants I, J). Then the elements of the 2-Selmer group of E are in one-to-one correspondence with $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes of locally soluble integral binary quartic forms having invariants equal to $2^4I, 2^6J$.*

Furthermore, the set of integral binary quartic forms that have a rational linear factor and invariants equal to 2^4I and 2^6J lie in one $\mathrm{PGL}_2(\mathbb{Q})$-equivalence class, and this class corresponds to the identity element in the 2-Selmer group of E.

We focus the rest of the talk on counting binary quartic forms.

Let $r_2(G)$ denote, for an arbitrary abelian 2-group G, the dimension of G over the finite field $\mathbb{F}_2$. The exact sequence gives us the equation

$$r_2(\mathrm{Sel}_2(E)) = \mathrm{rank}(E) + r_2(E(\mathbb{Q})[2]) + r_2(\text{Ш}_E[2]).$$

Note that

$$2r_2(\mathrm{Sel}_2(E)) \leq 2^{r_2(\mathrm{Sel}_2(E))} = \#\,\mathrm{Sel}_2(E),$$

thus the average size $\mathrm{Sel}_2(E)$ gives an upper bound for twice the rank. We now state the main theorem of Bhargava and Shankar

Theorem 2.3. *Sorting by naive height, we have*

$$\mathrm{Avg}\,\mathrm{Sel}_2(E) = 3.$$

This theorem is obtained by counting binary quartic forms having bounded invariants. A binary form is simply a homogeneous polynomial $f(x, y) \in \mathbb{Z}[x, y]$, where 'quartic' refers to its degree. The count is established by considering so-called co-regular representations of binary quartic forms, and counting integral orbits.

Definition 2.4. *A co-regular representation is a pair (G, V), where G is an algebraic group and V is a representation of G (both defined over $\mathbb{Z}$, say) such that the ring of relative polynomial invariants $G(\mathbb{C})$ on $V(\mathbb{C})$ is a polynomial ring.*

In our context, we will set $G = \mathrm{GL}_2$ and V is the vector space of binary quartic forms

$$\{ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 : a, b, c, d, e \in \mathbb{C}\}.$$

Gauss first considered the problem of counting binary quadratic forms in 1801. In this case, the 'ring of invariants' is generated by just one element, namely the discriminant $\Delta(f)$. The case of binary cubic forms was considered by Davenport and Heilbronn, and in that case the ring of invariants is also generated by just one element. However, in the quartic case, there are two independent invariants given by

$$I(f) = 12ae - 3bd + c^2,$$

$$J(f) = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$

In fact, these generated the ring of invariants of the action of $\mathrm{GL}_2(\mathbb{Z})$ on binary quartic forms. For instance, we have

$$\Delta(f) = (4I(f)^3 - J(f)^2)/27.$$

It turns out, due to work of Borel and Harish-Chandra, that for fixed values of I, J, both non-zero, there are only finitely many equivalence classes of integral binary quartic forms. Thus, if we set $h(I, J)$ to be the number of irreducible classes of binary quartic forms with invariants I, J, we can ask on average how many such equivalence classes there are as I, J vary.

Let us define another height which is qualitatively the same as our previous height for elliptic curves, but with different constants. Define

$$H(f) = H(I, J) = \max\{|I|^3, J^2/4\}.$$

They obtained the following theorem

Theorem 2.5. *Let $h^{(k)}(I, J)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of irreducible binary quartic forms having $4 - 2k$ real roots in $\mathbb{P}^1$ and invariants equal to I and J. Then*

(a) $\displaystyle\sum_{H(I,J)<X} h^{(0)}(I, J) = \frac{4}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon});$

(b) $\displaystyle\sum_{H(I,J)<X} h^{(1)}(I, J) = \frac{32}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon});$

(c) $\displaystyle\sum_{H(I,J)<X} h^{(2)}(I, J) = \frac{8}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon}).$

Let $V_{\mathbb{R}}$ denote the $\mathbb{R}$-vector space of binary quartic forms. We express an element $f \in V_{\mathbb{R}}$ in the form

$$f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4,$$

where $a, b, c, d, e \in \mathbb{R}$. Such an $f \in V_{\mathbb{R}}$ is said to be integral if $a, b, c, d, e \in \mathbb{Z}$. We aim to derive asymptotics for the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible integral binary quartic forms having bounded invariants. We also describe how these asymptotics change when we restrict to counting those binary quartic forms satisfying certain specified sets of congruence conditions.

The group $\mathrm{GL}_2(\mathbb{R})$ naturally acts on $V_{\mathbb{R}}$, namely via linear substitution. That is, for $\gamma \in \mathrm{GL}_2(\mathbb{R})$ we have the action

$$\gamma \cdot f(x,y) = f((x,y)\cdot\gamma).$$

This is a left action, meaning $(\gamma_1\gamma_2)\cdot f = \gamma_1 \cdot (\gamma_2 \cdot f)$.

We can also consider the action of $\mathrm{SL}_2^{\pm}(\mathbb{R})$ on $V_{\mathbb{R}}$, where $\mathrm{SL}_2^{\pm}(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R})$ is the subgroup of elements in $\mathrm{GL}_2(\mathbb{R})$ having determinant equal to ± 1. The ring of invariants for this action is generated by two independent generators of degrees 2 and 3, respectively, which are traditionally denoted by I and J. If

$$f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4,$$

then I, J are given by the two polynomial relations given previously. These are also relative invariants for the action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}$, since we have

$$I(\gamma\cdot f) = (\det\gamma)^4 I(f),$$
$$J(\gamma\cdot f) = (\det\gamma)^6 J(f).$$

The discriminant $\Delta(f)$ is a relative invariant of degree 6 is expressible in terms of I and J, namely

$$\Delta(f) = (4I(f)^3 - J(f)^2)/27.$$

The action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}$ preserves the lattice $V_{\mathbb{Z}}$ consisting of the integral elements of $V_{\mathbb{R}}$, and so we may ask: how many $\mathrm{GL}_2(\mathbb{Z})$-classes of forms are there having height at most X? More precisely, we may ask: how many $\mathrm{GL}_2(\mathbb{Z})$-classes of forms are there with height at most X and a given number of real roots?

A simple device coming from complex analysis and the theory of modular forms is the notion of fundamental domains. By a fundamental domain we mean a subset D of our vector space $V_{\mathbb{R}}$ such that every element of $V_{\mathbb{R}}$ can be obtained from a point in D via a $\mathrm{GL}_2(\mathbb{R})$-action. Unfortunately, these fundamental domains are not bounded, which is a crucial feature when one wants to apply a geometry of numbers type argument (indeed, the fundamental domain for counting points in a lattice is simply the fundamental parallelepiped, which is obviously compact). Instead, these fundamental domains have intransigent cusps which may have large volume.

In the next talk we will define the fundamental domain and continue our quest to count binary quartic forms with bounded invariants.

3. Binary quartic forms and average ranks of elliptic curves (2/3) by Stanley Xiao

In the last talk we showed the following:

(a) Bounding the rank of an elliptic curve $E/\mathbb{Q}$ can be done by bounding the size of the 2-Selmer group $\mathrm{Sel}_2(E)$;
(b) Bounding $\# \mathrm{Sel}_2(E)$ can be done by counting binary quartic forms;
(c) The space of real binary quartic forms is acted upon by $\mathrm{GL}_2(\mathbb{R})$; and
(d) We can define some nice fundamental domain of the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}$ to facilitate the counting problem.

The basic idea of the geometry of numbers is that we can compare the number of lattice points (say, in $\mathbb{Z}^r$ for some $r \geq 1$) in a homogeneously expanding region to the volume of the region, as it grows with respect to the homogeneously expanding parameter X, say. We can visualize the set of binary quartic forms with integer coefficients as a lattice isomorphic to $\mathbb{Z}^5$ sitting in $\mathbb{R}^5$. However, since we are sorting them by a rather strange height (namely $H(f) = H(I,J) = \max\{|I|^3, J^2/4\}$), the problem is not as simple. Further, we have to account for over-counting $\mathrm{GL}_2(\mathbb{Z})$-equivalent forms. Thus it is $\mathrm{GL}_2(\mathbb{Z})$-action, not simply a homogeneously expanding group action, which is relevant. This produces many difficulties.

In this talk our aim is to give some convenient fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}$. The main difficulty is that these domains tend to have cusps, which may have very large volume. Success will come when we show that while the cusps may have large volume, they only contain reducible points.

For $j = 0, 1, 2$ denote $V_{\mathbb{R}}^{(j)}$ to be the set of binary quartic forms with $4-2j$ real roots. In particular, $V_{\mathbb{R}}^{(2)}$) consists of <u>definite</u> quartic forms; namely those which are always positive or always negative. In this case, let $V_{\mathbb{R}}^{(\pm 2)}$ to be the set of binary quartic forms in $V_{\mathbb{R}}^{(2)}$ which are always positive or negative, respectively. Analogously, define $V_{\mathbb{Z}}^{(j)} = V_{\mathbb{R}}^{(j)} \cap V_{\mathbb{Z}}$. The following are two important facts about binary quartic forms:

- The set of binary quartic forms in $V_{\mathbb{R}}$ having fixed invariants I and J consists of just one $\mathrm{SL}_2^{\pm}(\mathbb{R})$-orbit if $4I^3 - J^2 < 0$; this orbit lies in $V_{\mathbb{R}}^{(1)}$.
- The set of binary quartic forms in $V_{\mathbb{R}}$ having fixed invariants I and J consists of three $\mathrm{SL}_2^{\pm}(\mathbb{R})$-orbits if $4I^3 - J^2 > 0$; in this case, there is one such orbit in each of $V_{\mathbb{R}}^{(0)}, V_{\mathbb{R}}^{(2+)}, V_{\mathbb{R}}^{(2-)}$.

Since $I(g\cdot f) = (\det g)^4 I(f)$ and $J(g \cdot f) = (\det g)^6 J(f)$, it follows that two forms $f_1, f_2 \in V_{\mathbb{R}}^{(j)}$ are $\mathrm{GL}_2(\mathbb{R})$-equivalent if and only if there exists a positive constant $\lambda \in \mathbb{R}$ with $I(f_1) = \lambda^2 I(f_2)$ and $J(f_1) = \lambda^3 J(f_2)$. For $(I,J) \neq (0,0)$, there exists a $\lambda \in \mathbb{R}$ such that

$$H(\lambda^2 I, \lambda^3 J) = \max\{\lambda^6 |I|^3, \lambda^6 J^2/4\} = 1.$$

Hence for $j = 0, 2+, 2-$ (respectively for $j = 1$), a fundamental set $L^{(j)}$ for the action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}^{(i)}$ can be constructed by choosing one form $f \in V_{\mathbb{R}}^{(i)}$, having invariants I and J, for each (I,J) such that $H(I,J) = 1$ and $4I^3 - J^2 > 0$ (respectively $4I^3 - J^2 < 0$). The list is below:

$$L^{(0)} = \left\{ x^3 y - \frac{1}{3} x y^3 - \frac{J}{27} y^4 : -2 < J < 2 \right\},$$

$$L^{(1)} = \left\{x^3y - \frac{I}{3}xy^3 + \frac{\pm 2}{27}y^4 : -1 \leq I < 1\right\} \cup \left\{x^3y + \frac{1}{3}xy^3 - \frac{J}{27}y^4 : -2 < J < 2\right\},$$
$$L^{(2+)} = \left\{\frac{1}{16}x^4 - \frac{\sqrt{2-J}}{3\sqrt{3}}x^3y + \frac{1}{2}x^2y^2 + y^4 : -2 < J < 2\right\},$$
$$L^{(2-)} = \left\{f : -f \in L^{(2+)}\right\}.$$

Note that these fundamental sets $L^{(j)}$ all have the property that the coefficients of the binary quartic forms in them have bounded coefficients. Now for any fixed compact subset $G_0 \subset \mathrm{GL}_2(\mathbb{R})$ and any $h \in G_0$, the set $h \cdot L^{(i)}$ is also a fundamental set for the action of $\mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}^{(i)}$, and all coefficients are then bounded independent of h. We note the following lemma, which we will not prove:

Lemma 3.1. *Let f be an element of $V_{\mathbb{R}}^{(j)}$ having non-zero discriminant. Then the order of the stabilizer of f in $\mathrm{GL}_2(\mathbb{R})$ is 8 if $j = 0, 2$ and 4 if $j = 1$.*

Now let $\mathcal{F}$ denote Gauss's usual fundamental domain for $\mathrm{GL}_2(\mathbb{Z}) \setminus \mathrm{GL}_2(\mathbb{R})$ in $\mathrm{GL}_2(\mathbb{R})$. We have the following Iwasawa decomposition for $\mathcal{F}$, namely

$$\mathcal{F} = \{n\alpha k\lambda : n(u) \in N'(t), \alpha(t) \in A', k \in K, \lambda \in \Lambda\}$$

where

$$N'(t) = \left\{\begin{pmatrix} 1 & \\ u & 1\end{pmatrix} : u \in \nu(t)\right\}, A' = \left\{\begin{pmatrix} t^{-1} & \\ & t\end{pmatrix} : t \geq (3/4)^{1/4}\right\},$$
$$\Lambda = \left\{\begin{pmatrix} \lambda & \\ & \lambda\end{pmatrix} : \lambda > 0\right\}$$

and K is the real orthogonal group $\mathrm{SO}_2(\mathbb{R})$. Here $\nu(t)$ is a union of on or two subintervals of $\left[\frac{-1}{2}, \frac{1}{2}\right]$ depending only on the value of t. These should be clear from the diagram.

For $j = 0, 1, 2+$ and $2-$, let $2n_j$ denote the cardinality of the stabilizer in $\mathrm{GL}_2(\mathbb{R})$ of an irreducible element $v \in V_{\mathbb{R}}^{(j)}$. Then, by Lemma 3.1 we have $n_0 = 4, n_1 = 2, n_{2+} = 4$, and $n_{2-} = 4$. For each $h \in \mathrm{GL}_2(\mathbb{R})$, we regard $\mathcal{F}h \cdot L^{(j)}$ as a multiset, where the multiplicity of a point $x \in \mathcal{F}h \cdot L^{(j)}$ is given by the cardinality of the set

$$\{g \in \mathcal{F} : x \in gh \cdot L^{(j)}\}.$$

We claim that the $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of $x \in V_{\mathbb{R}}^{(j)}$ is represented

$$m(x) = \#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x)/\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x)$$

times in the multiset $\mathcal{F}h \cdot L^{(j)}$. That is, the multiplicity of x' in $\mathcal{F}h \cdot L^{(j)}$, summed over all $x' \in V_{\mathbb{Z}}$ that are $\mathrm{GL}_2(\mathbb{Z})$-equivalent to x, is equal to $m(x)$. Indeed, for any element $x \in V_{\mathbb{R}}^{(i)}$, there exists a unique element $x_L \in h \cdot L^{(i)}$ that is $\mathrm{GL}_2(\mathbb{R})$-equivalent to x. Suppose $g \in \mathrm{GL}_2(\mathbb{R})$ satisfies $g \cdot x_L = x$. Then for an element $g' \in \mathrm{GL}_2(\mathbb{R})$, the element $g' \cdot x_L \in V_{\mathbb{Z}}$ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to x if and only if $g' = \gamma g g_0$ for some $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ and $g_0 \in \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x_L)$, that is, if and only if g and g' map to the same element in the double coset space

$$\mathrm{GL}_2(\mathbb{Z}) \setminus \mathrm{GL}_2(\mathbb{R}) / \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x_L).$$

The number of such double cosets in the single right coset $\mathrm{GL}_2(\mathbb{Z})g$ is equal to

$$\frac{\#[g\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x_L)g^{-1}}{\#[\mathrm{GL}_2(\mathbb{Z})\cap g\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x_L)g^{-1}]}=\frac{\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})(x)}}{\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x)}=m(x)$$

as desired.

Since the stabilizer in $\mathrm{GL}_2(\mathbb{Z})$ of an element $x \in V_{\mathbb{R}}$ always contains the identity and its negative, $m(x)$ is always a number between 1 and n_j. In fact, for almost all $x \in V_{\mathbb{R}}^{(j)}$, the quantity $m(x)$ is equal to n_i. Indeed, for any fixed $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ not equal to plus or minus the identity, the set of elements in $V_{\mathbb{R}}$ that are fixed by γ has measure zero (with respect to Lebesgue measure). Since $\mathrm{GL}_2(\mathbb{Z})$ is countable, it follows that the set of elements $x \in V_{\mathbb{R}}^{(j)}$ such that $m(x) < n_j$ also has measure 0. Thus for any $h \in \mathrm{GL}_2(\mathbb{R})$, away from a null set, the multiset $\mathcal{F}h \cdot L^{(j)}$ is the union of n_j fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}^{(j)}$.

Thus, for any $h \in \mathrm{GL}_2(\mathbb{R})$, if we let $\mathcal{R}_X(h \cdot L^{(i)})$ denote the multiset $\{w \in \mathcal{F}h \cdot L^{(j)} : |H(w)| < X\}$, then the product $n_j\mathcal{R}_X(h \cdot L^{(j)})$, with the slight caveat that the (relatively rate) points with $\mathrm{GL}_2(\mathbb{Z})$-stabilizers of cardinality $2r(r > 1)$ are counted with weight $1/r$.

As mentioned before, the main obstacle to counting integral points in this region $\mathcal{R}_X(h \cdot L^{(j)})$ is that it is not bounded, but rather has a cusp going off to infinity (namely, the part of $\mathcal{R}_X(h \cdot L^{(j)})$ where the first coordinate a becomes small in absolute value, or equivalently, where the parameter t in the subgroup $A' < \mathrm{GL}_2(\mathbb{R})$ can tend to infinity. This leads to forms with arbitrarily small first coefficient a. This can be dealt with via a method called “thickening" the cusp; more precisely, we compute the number of integral points in the region $\mathcal{R}_X(h \cdot L^{(j)})$ by averaging over a “compact continuum" of such fundamental regions, i.e., by averaging over the domains $\mathcal{R}_X(h \cdot L^{(j)})$ where h ranges over a certain compact subset $G_0 \subset \mathrm{GL}_2(\mathbb{R})$. But first, we move to bounding the number of reducible points in the main bodies (i.e. away from the cusps) of our fundamental regions.

We consider the integral elements in the multiset $\mathcal{R}_X(h \cdot L^{(j)})$ that are reducible over $\mathbb{Q}$, where h is any element in a fixed compact subset G_0 of $\mathrm{GL}_2(\mathbb{R})$. Note that if a binary quartic form $ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ satisfies $a = 0$ (so that, in particular, it lies in the cusp of the region $\mathcal{R}_X(h \cdot L^{(j)})$, then it is automatically reducible over $\mathbb{Q}$ since y is a factor. The following lemma shows that for integral binary quartic forms in $\mathcal{R}_X(h \cdot L^{(j)})$, reducibility with $a \neq 0$ does not occur very often (i.e. there are a negligible number of reducible points in the main body of the fundamental domain). This will be covered in the next talk.

4. Binary quartic forms and average ranks of elliptic curves (3/3) by Stanley Xiao

Our first goal in this talk is to prove the following lemma in [2]:

Lemma 4.1. *Let $h \in G_0$ be any element, where G_0 is any fixed compact subset of $\mathrm{GL}_2(\mathbb{R})$. Then the number of integral binary quartic forms $ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \in \mathcal{R}_X(h \cdot L^{(j)})$ that are reducible over $\mathbb{Q}$ with $a \neq 0$ is $O(X^{2/3+\varepsilon})$, where the implied constant depends only on G_0 and ε.*

Proof. Let $f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ be any element in $\mathcal{R}_X(h \cdot L^{(j)})$. We know that $\mathcal{R}_X(h \cdot L^{(j)}) \subset N'A'K\Lambda h \cdot L^{(j)}$, where $h \cdot L^{(j)}$ lies in a fixed compact set and $0 < \lambda < X^{1/24}$. Since all the coefficients of all the elements in $K\Lambda h \cdot L^{(j)}$ are bounded by $O((X^{1/24})^4) = O(X^{1/6})$, it follows that in $N'A'K\Lambda h \cdot L^{(j)}$, we still have $a = O(X^{1/6}), b = O(X^{1/6}), c = O(X^{1/6}), ad = O(X^{2/6}), bd = O(X^{2/6})$, and $ae = O(X^{2/6})$. This is because N' cannot grow the coefficients too much, as the parameter u in N' is bounded by $1/2$. A' then is the only thing that can grow the coefficients out of bounds, but in such a way so that products of coefficients cannot grow too much as indicated above. These latter estimates clearly imply that the number of points n $\mathcal{R}_X(h \cdot L^{(j)})$ with $a \neq 0$ and $e = 0$ is $O(X^{4/6+\varepsilon})$.

If $a \neq 0$ and $e \neq 0$, then it should be really hard for $f(x,y)$ to be reducible. We first estimate the number of forms that have a rational linear factor. The previous estimates show that the number of possibilities for the quadruple (a,b,d,e) is at most $O(X^{4/6+\varepsilon})$. If $px + qy$ is a linear factor of $f(x,y)$, where $p, q \in \mathbb{Z}$ are relatively prime, then p must be a factor of a while q must be a factor of e; they are thus both determined up to $O(X^\varepsilon)$ possibilities. Once p and q are determined, computing $f(-q,p)$ and setting it equal to zero then uniquely determines c (if it is an integer at all) in terms of a,b,d,e,p,q. Thus the total number of forms $f \in \mathcal{R}_X(h \cdot L^{(j)})$ having a rational linear factor and $a \neq 0$ is $O(X^{4/6+\varepsilon})$.

We now estimate the number of binary quartic forms in $\mathcal{R}_X(h \cdot L^{(j)})$ that factor into two irreducible binary quadratic forms over $\mathbb{Z}$, say

$$ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 = (px^2 = qxy + ry^2)\left(\frac{a}{p}x^2 + sxy + \frac{e}{r}y^2\right)$$

where $p,q,r,s \in \mathbb{Z}$ and p,q,r are relatively prime. Since $ae = O(X^{2/6})$ and $a, e \neq 0$, the number of possibilities for the pair (a,e) is $O(X^{2/6+\varepsilon})$. We then see that p divides a and r divides e, and hence the number of possibilities for (p,r), once a and e have been fixed, is bounded by $O(X^\varepsilon)$.

Equating coefficients, we see that

$$\frac{a}{p}q + ps = b,$$
$$\frac{e}{r}q + rs = d.$$

There are two cases. We first consider the case where $\frac{ar}{pe} \neq \frac{p}{r}$, i.e., the above linear system in the variables q and s is non-singular. Then the values of b and d uniquely determine q and s, and so the total number of quadruples (a,b,d,e), and thus the total number of octuples (a,b,d,e,p,r,q,s), is at most $O(X^{4/6+\varepsilon})$. Furthermore, once this octuple has been fixed, this also then determines c by equating coefficients of x^2y^2. Hence there are at most $O(X^{4/6+\varepsilon})$ possibilities for (a, b, c, d, e) in this case.

Next we consider the case where $\frac{ar}{pe} = \frac{p}{r}$, so that the system is singular. In this case, the value of b determines the value of d uniquely; namely, $d = (r/p)b$. We have already seen that there are $O(X^{2/6+\varepsilon})$ possibilities for the quadruple (a, e, p, r). Since there are only $O(X^{1/6})$ choices for each of b and c, and then d is determined by b, the total number of choices for (a, b, c, d, e) is again $O(X^{4/6+\varepsilon})$, as desired. □

The next lemma states that those points with large stabilizers are rare. We will not give the proof in these talks.

Lemma 4.2. *The number of* $\mathrm{GL}_2(\mathbb{Z})$*-orbits of integral binary quartic forms* $f \in V_{\mathbb{Z}}$ *such that* $\Delta(f) \neq 0$ *and* $H(f) < X$ *whose stabilizer in* $\mathrm{GL}_2(\mathbb{Q})$ *has size greater than* 2 *is* $O(X^{3/4+\varepsilon})$.

5. Ternary cubic forms with bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0

by Stanley Yao Xiao

6. Most curves satisfy the BSD by Stanley Yao Xiao

7. Most hyperelliptic curves have no rational points
by Stanley Yao Xiao

8. Most odd degree hyperelliptic curves have exactly one rational point
by Stanley Yao Xiao

References

[1] M. Bhargava, Most hyperelliptic curves over Q have no rational points, `http://arxiv.org/abs/1308.0395`

[2] M. Bhargava, A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, Annals of Mathematics **181** (2015), 191-242.

[3] M. Bhargava, A. Shankar, Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, Annals of Mathematics **181** (2015), 587-621.

[4] M. Bhargava, A. Shankar, The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1, `http://arxiv.org/abs/1312.7859`

[5] B. Poonen, M. Stoll, Most odd degree hyperelliptic curves have only one rational point, Annals of Mathematics **180** (2014), 1137-1166.

[6] A. Shankar, X. Wang, Average size of the 2-Selmer group of Jacobians of monic even hyperelliptic curves, `http://arxiv.org/abs/1307.3531`.