AVERAGE RANKS OF ELLIPTIC CURVES

BASED ON MINI-COURSE BY PROF. TIM DOKCHITSER

ADAM MICKIEWICZ UNIVERSITY IN POZNAŃ, 14 – 16.05.2014,
NOTES TAKEN BY JĘDRZEJ GARNEK

Contents

Introduction

Rational points and ranks of elliptic curves are subjects of many important conjectures, such as the Birch-Swinnerton-Dyer conjecture and conjectures on 'typical' and 'maximal' ranks. In a recent series of papers, Manjul Bhargava and his collaborators made several fundamental breakthroughs on average ranks and Selmer ranks of elliptic curves over the rationals. In particular, they prove that the average rank of all elliptic curves over $\mathbb{Q}$ is less than 1, and deduce that a positive proportion of elliptic curves satisfy the Birch-Swinnerton-Dyer conjecture. This beautiful work combines techniques from invariant theory, Selmer groups, geometry and analytic number theory. The goal of the mini-course was to give a brief and quite elementary overview of these results, and to give an introduction to some of the ingredients of the proofs.

1. Diophantine equations

The main field of interest of arithmetic geometry are the so-called **algebraic varieties**, i.e. sets of solutions of systems of equations of the form

$$V : \begin{cases} f_1(x_1, \ldots, x_n) &= 0 \\ \cdots & \\ f_k(x_1, \ldots, x_n) &= 0 \end{cases}$$

where $f_i \in K[x_1, \ldots, x_n]$ are polynomials with coefficients in a fixed field K (in these lectures we will be interested mostly in the case $K = \mathbb{Q}$, and have f_i with $\mathbb{Z}$-coefficients). We say that V is *defined over* K and write V/K to denote it. Let $V(K)$ denote the set of K – *rational points* on V, i.e. $V(K) = \{(a_1, \ldots, a_n) \in K^n : f_i(a_1, \ldots, a_n) = 0,\ i = 1, \ldots, k\}$; analogously we define sets $V(\mathbb{Z})$, $V(\mathbb{C})$, $V(\mathbb{F}_p)$, etc.
Given an algebraic variety $V/\mathbb{Q}$ we will be interested in the following questions:

Question 1: Is $V(\mathbb{Q})$ empty? Is $V(\mathbb{Z})$ empty?

Question 2: Is $V(\mathbb{Q})$ infinite?

Question 3: How does $\#\{P \in V(\mathbb{Q}) : H(P) < c\}$ grows with $c \to \infty$?
(H denotes a height function, measuring the "complexity" of points)

In full generality, all three questions are extremely hard. The problem of determining if $V(\mathbb{Z}) \neq \varnothing$ is known as **Hilbert's tenth problem** and is proven to be undecidable – there exists no algorithm that given any variety $V/\mathbb{Q}$ decides, if it has any integral points. Poonen showed that if the answer to the following question is affirmative, then the first part of **Question 1** is also undecidable:

Question 1.1. *There exists a $V/\mathbb{Q}$ and a rational map $g : V \to \mathbb{Q}$ such that $g(V(\mathbb{Q}))$ is infinite and discrete.*

In the lectures we will focus on the "well–understood" case of algebraic varieties, i.e. curves.

2. Curves

With an algebraic variety V/K given as above we can associate its **field of rational functions**:

$$K(V) := \text{ field of fractions of } K[x_1, \ldots, x_k]/\langle f_1, \ldots, f_k \rangle$$

The **dimension** of the variety is definied as the transcendence degree of the extension $K(V)/K$ (i.e. the cardinality of maximal subset of $K(V)$ that doesn't satisfy any polynomial with coefficients in K).

A **curve** is a projective algebraic variety of dimension 1; for simplicity all considered curves will be smooth and absolutely irreducible (i.e. we can not decompose it as a union of two algebraic sets in $\overline{K}$).
Note that $C(\mathbb{C})$ is a Riemann surface and can be viewed as a two-dimensional, compact, orientable manifold. By the **classification theorem of surfaces**, any such manifold is made of some finite number g of "glued" tori; this number is defined to be the **genus** of the curve; it determines many geometric and arithmetic properties of the curve.

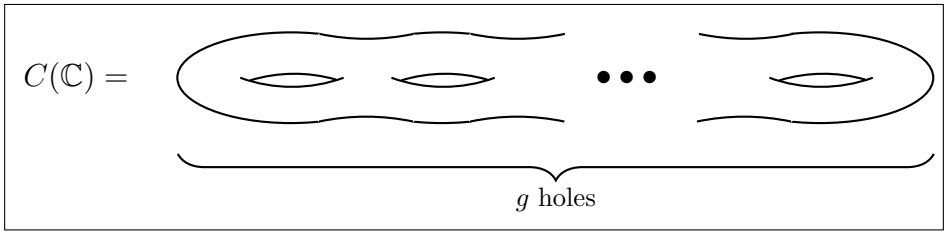


FIGURE 1. The genus of a curve

In particular, the answer to the **Questions 1,2,3** depends on genus:

- if $g = 0$, then C is a line or a conic and $C(\mathbb{Q})$ is either empty or infinite.

  Exercise 1. Suppose $C : ax^2 + by^2 = c$ $(a, b, c \in \mathbb{Q})$ is a conic. Prove that either $C(\mathbb{Q}) = \varnothing$ or $C(\mathbb{Q})$ is infinite.

  Moreover, we have a method of determining, which one of these two possibilities occurs:

  Theorem 2.1. *(Hasse–Minkowski)*
  If $C : F(x, y) = 0$ is a conic over $\mathbb{Q}$, then $C(\mathbb{Q}) \neq \varnothing$ iff $C(\mathbb{R}) \neq \varnothing$ and for all prime p: $C(\mathbb{Q}_p) \neq \varnothing$ (i.e. $F(x, y) = 0$ has solutions $\pmod{p^n}$ for all n).

  Exercise 2. Prove that for $C : x^2 + y^2 = 3$ we have $C(\mathbb{Q}) = \varnothing$.

  In other words we can say that C is **soluble** (i.e. has a rational point) if and only if it's **locally soluble** (i.e. has a point in every completion of $\mathbb{Q}$). This theorem, also known as **the local–global principle**, fails for curves of higher genus, as shown by Selmer – the curve $3x^3 + 4y^3 = 5$ is locally soluble, but has no rational points. We'll come across this problem in section 5.

- if $g = 1$ and $C(\mathbb{Q}) \neq \varnothing$ then C is called **an elliptic curve**. Otherwise, if $C(\mathbb{Q}) = \varnothing$ then there exists an elliptic curve E (the Jacobian of C) such that C and E are isomorphic over $\overline{\mathbb{Q}}$.

- if $g \geq 2$ then the following theorem gives us an answer to the **Question 2**:

  Theorem 2.2. *(Faltings, 1983) If genus of a curve C over $\mathbb{Q}$ is ≥ 2 then $C(\mathbb{Q})$ is finite.*

In the next sections we'll study the genus one case closer.

3. Elliptic curves – models and group structure

Theorem 3.1. *If* $\operatorname{char} K \neq 2, 3$ *then any elliptic curve E/K can be embedded in $\mathbb{P}^2(K)$ as a plane cubic with an equation of the form $y^2 = x^3 + Ax + B$, where $A, B \in K$ and $\Delta := 16(4A^3 + 27B^2) \neq 0$. This equation is unique up to change of variables $(A, B) \mapsto (t^4 A, t^6 B)$, $t \in K^\times$. Conversely, any curve of this form is an elliptic curve.*

Proof (sketch):
Let's pick any point $\mathcal{O} \in E(K)$.
For any curve C/K and $\mathcal{O} \in C(K)$ we can consider the K-linear subspace of the function field $K(C)$:

$$\mathcal{L}(n\mathcal{O}) := \{f \in K(C) : f \text{ has a pole of order at most } n \text{ at } \mathcal{O} \text{ and no other poles}\}$$

It turns out, that the dimension of $\mathcal{L}(n\mathcal{O})$ equals $n - genus(C) + 1$ for $n \geq 2g - 1$ (**the Riemann–Roch theorem**) – thus, in the case of elliptic curves: $\dim \mathcal{L}(n\mathcal{O}) = n$ for any $n \geq 1$. Let's have a look at $\mathcal{L}(n\mathcal{O})$ for small n. For $n = 1$ we have $\dim \mathcal{L}(\mathcal{O}) = 1$ and thus $\mathcal{L}(\mathcal{O}) = \langle 1 \rangle$ (the constant functions have no pole at $\mathcal{O}$). Then, since $\dim \mathcal{L}(2\mathcal{O}) = 2$, we must have $\mathcal{L}(2\mathcal{O}) = \langle 1 \rangle \oplus \langle x \rangle$ for some function $x \in K(E)$ with pole of order 2 in $\mathcal{O}$. Analogously, we have $\mathcal{L}(2\mathcal{O}) = \langle 1 \rangle \oplus \langle x \rangle \oplus \langle y \rangle$ for some $y \in K(E)$ with pole of order 3. Then the seven functions: $1, x, y, x^2, xy, x^3, y^2$ belong to the 6 dimensional space $\mathcal{L}(6\mathcal{O})$. Thus we must have a K-linear relation between them; the analysis of order at $\mathcal{O}$ shows also that the coefficients by y^3 and x^3 sum to 0. In this way we obtain a relation of the form: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for $a_1, \ldots, a_6 \in K$. After shifting x and y (here we use $\operatorname{char} K \neq 2, 3$) we obtain the desired short Weierstrass form $y^2 = x^3 + Ax + B$. One shows that $P \mapsto [x(P) : y(P) : 1]$ is an embedding of E into $\mathbb{P}^2(K)$. The converse theorem follows for example from **Plücker genus formula**. □

As pointed out by Poincaré, $E(K)$ has a structure of an abelian group.

In case of $K = \mathbb{R}$ we can describe the addition of points geometrically: given points P, Q on curve $E : y^2 = x^3 + Ax + B$ we draw a line L through P and Q (if $P = Q$ we draw a tangent at P) and denote by R the third point of intersection of L and E. Then $P + Q$ is defined to be R reflected through x-axis. The neutral element is $\mathcal{O} = [0 : 1 : 0]$ ("the point in infinity") and the inverse element of a point P is defined to be its reflection through x-axis. Thus for $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, $P \neq \pm Q$ we have $P + Q = (x_3, y_3)$ where

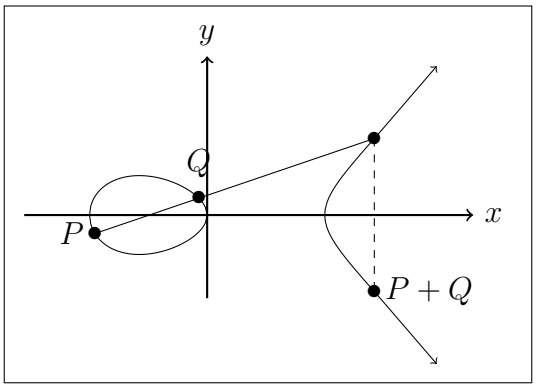


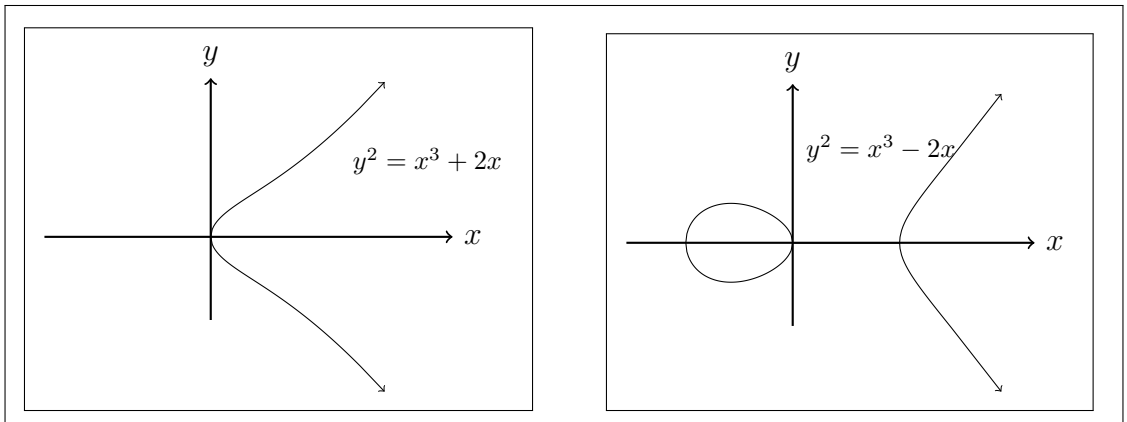
FIGURE 2. Addition law on an elliptic curve

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \qquad y_3 = -\frac{y_2 - y_1}{x_2 - x_1}x_3 - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

This group law seems to be complicated, however what is most important, the addition of points is given by rational functions in coordinates of the points and E is an algebraic group. Note that these formulas define the group law for an arbitrary field K. For $K = \mathbb{R}$ or $\mathbb{C}$ it is easy to describe structure of $E(K)$:

- $E(\mathbb{C}) \cong S^1 \times S^1$ is a complex torus (note that $E(\mathbb{C})$ must be homeomorphic to torus, as it a Riemann surface of genus 1),
- $E(\mathbb{R})$ is a compact Lie group with one or two components (depending on sign of Δ). The only compact and connected Lie group is S^1, thus

$$E(\mathbb{R}) \cong \begin{cases} S^1, & \Delta < 0 \\ S^1 \times \mathbb{Z}/2, & \Delta > 0 \end{cases}$$



(a) $\Delta < 0 \Rightarrow E(\mathbb{R}) \cong S^1$ (b) $\Delta > 0 \Rightarrow E(\mathbb{R}) \cong S^1 \times \mathbb{Z}/2$

FIGURE 3. Structure of $E(\mathbb{R})$

The question about structure of $E(K)$ when K is a number field was solved by Mordell and Weil:

Theorem 3.2. *(Mordell–Weil) If K is a number field and E/K an elliptic curve, then $E(K)$ is a finitely generated abelian group, i.e. it is of the form:*

$$E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r$$

where $E(K)_{tors}$ is a finite subgroup of torsion elements.
The number r is called ***the rank of the curve*** *over K and is denoted by* $\operatorname{rk} E/K$.

Proof (overview):
The proof consists of two steps:

1) **"the weak Mordell–Weil theorem"**: one shows that for some $n > 1$ (usually $n = 2$) the group $E(K)/nE(K)$ is finite: $E(K)/nE(K) = \{[Q_1], \ldots, [Q_r]\}$,

2) **"the descent argument"**: one considers the height function $h : E(K) \to \mathbb{R}$ – in the case of in the case $K = \mathbb{Q}$ it's given by:

$$h(P) = \log \max\{ \text{ numerator of } x(P), \text{ denominator of } x(P)\}$$

and shows that it has the following properties:

(i) for any $Q \in E(K)$ there is a constant $C_Q > 0$ (depending on E and Q) such that $h(P + Q) \leq 2h(P) + C_Q$ for all $P \in E(K)$,

(ii) for any $n \geq 2$ there exists a constant $D_n > 0$ (depending on E and n) such that $h(nP) \geq n^2 h(P) - D_n$ for all $P \in E(K)$,

(iii) for every constant $C > 0$ the set $\{P \in E(K) : h(P) \leq C\}$ is finite.

Then it's possible to show that the set:

$$\{Q_1, \ldots, Q_r\} \cup \left\{ Q \in E(K) : h(Q) \leq 1 + \frac{1}{2}(C + D_n) \right\}$$

(where $C = \max\{C_{-Q_i} : i = 1, \ldots, r\}$) generates $E(K)$.

□

The proof of Mordell–Weil theorem shows that finding generators of $E(\mathbb{Q})$ comes down to determining generators of $E(\mathbb{Q})/nE(\mathbb{Q})$ for any n. Unfortunately, as of today there is no known procedure that is guaranteed to give generators for this group. However, the torsion subgroup of $E(\mathbb{Q})$ is well-understood and for any given curve it can be easily found by using the following theorems:

Theorem 3.3. *(Lutz–Nagell) If $E : y^2 = x^3 + Ax + B$ $(A, B \in \mathbb{Z})$ is an elliptic curve and $P = (x, y) \in E(\mathbb{Q})$ is a torsion element, then $x, y \in \mathbb{Z}$ and we have: $y = 0$ (equivalently $[2]P = \mathcal{O}$) or $y^2 | \Delta$.*

Theorem 3.4. *Let $E : y^2 = x^3 + Ax + B$, $(A, B \in \mathbb{Z})$ be an elliptic curve and let's consider its reduction $\pmod p$ for a prime $p \nmid \Delta$: $\widetilde{E}(\mathbb{F}_p) : y^2 = x^3 + \widetilde{A}x + \widetilde{B}$ (the tilde denotes reduction $\pmod p$). Then the reduction map $E(\mathbb{Q}) \to \widetilde{E}(\mathbb{F}_p)$, $(x, y) \mapsto (\widetilde{x}, \widetilde{y})$ is a homomorphism. Thus, (by Lutz–Nagell theorem) it is injective on torsion points.*

Exercise 3. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + 1$.

(a) find 6 rational points on E and show that they generate a 6-element cyclic subgroup of $E(\mathbb{Q})$,
(b) use the two previous theorems to find $E(\mathbb{Q})_{tors}$.

Theorem 3.5. *(Mazur) The group $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups: $\mathbb{Z}/N\mathbb{Z}$ for $N \in \{1, 2, \ldots, 10, 12\}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $N \in \{1, 2, 3, 4\}$. Conversely, each of this groups is isomorphic to $E(\mathbb{Q})_{tors}$ for some elliptic curve $E/\mathbb{Q}$.*

It turns out that finding generators of $E(\mathbb{Q})/nE(\mathbb{Q})$ comes down to finding rational points on some special curves (the so-called **Selmer Curves**); however the failure of Hasse principle makes this procedure difficult. We don't know which integers can occur as rank of an elliptic curve over $\mathbb{Q}$ or whether the rank over $\mathbb{Q}$ is bounded. We mention two more conjectures concerning rank in the family of quadratic twists of a given elliptic curve:

Definition 3.1. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$. Then for any $d \in \mathbb{Q}^\times$ we can define its **quadratic twist** by d as the curve: $E_d : dy^2 = x^3 + Ax + B$ or equivalently $E_d : y^2 = x^3 + Ad^2x + Bd^3$ (note that E and E_d are isomorphic over $\overline{\mathbb{Q}}$, but not over $\mathbb{Q}$).*

Conjecture 3.6. *For any $E/\mathbb{Q}$ the set $\{\operatorname{rk} E_d/\mathbb{Q} : d \in \mathbb{Q}^\times\}$ is unbounded.*

Conjecture 3.7. *(Honda, Granville, Watkins) For any $E/\mathbb{Q}$ there are only finitely many $d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ such that $\operatorname{rk} E_d/\mathbb{Q} > 9$.*

Note that the two conjectures contradict each other!

Exercise 4. Find injections $E(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}(\sqrt{d}))$ and $E_d(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}(\sqrt{d}))$. Prove that $\operatorname{rk} E/\mathbb{Q}(\sqrt{d}) = \operatorname{rk} E/\mathbb{Q} + \operatorname{rk} E_d/\mathbb{Q}$.

Exercise 5. Let $K/\mathbb{Q}$ be an odd degree Galois extension. Show that $\operatorname{rk} E/K \equiv \operatorname{rk} E/\mathbb{Q} \pmod 2$.

The largest known rank is 28 (an example was given by Noam Elkies). It is conjectured that the rank is unbounded; however, as shown by Bhargava–Shankar, the average rank of all elliptic curves over $\mathbb{Q}$ is < 1. To define what average rank means, we need to order the curves by height. Note that every elliptic curve $E/\mathbb{Q}$ has a unique representation in the form $y^2 = x^3 + Ax + B$ for $A, B \in \mathbb{Z}$ such that $\forall_p \quad p^4 \nmid A$ or $p^6 \nmid B$.

Definition 3.2. *For $E = E_{A,B} : y^2 = x^3 + Ax + B$ $(A, B \in \mathbb{Z})$ we define its* ***height*** *as $H_E = H_{A,B} = \max\{4|A|^3, 27B^2\}$.*
Let us denote $\mathcal{E} := \{E_{A,B} : A, B \in \mathbb{Z}, 4A^3 + 27B^2, \forall_p \quad p^4 \nmid A, p^6 \nmid B\}$. We say that the density of a set $F \subset \mathcal{E}$ is equal to α if:

$$\lim_{X\to\infty} \frac{\#\{E \in F : H_E < X\}}{\#\{E \in \mathcal{E} : H_E < X\}} = \alpha$$

Example 3.8.

(1) if $F \subset \mathcal{E}$ is a set of elliptic curves satisfying finitely many congruence conditions on A, B (eg. $A \equiv 1 \pmod 5$) then F has positive proportion.
(2) 100% of elliptic curves/$\mathbb{Q}$ have $E(\mathbb{Q})_{tors} = \{\mathcal{O}\}$ (by Mazur's theorem it suffices to prove that 100% of elliptic curves has no 2-, 3-, 5-, 7- tosion points).

Exercise 6. Prove that for 100% of elliptic curves/$\mathbb{Q}$: $E(\mathbb{Q})[2] = \{\mathcal{O}\}$.

4. BSD Conjecture

With every elliptic curve $E/\mathbb{Q}$ we can associate its L–function, defined as a product of local factors. It is given in a form of a Dirichlet series: $L(E, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ (the series is convergent for $Re\, s > \frac{3}{2}$). It turns out that every such L-function comes from a modular form and thus shares properties of L-functions associated with modular forms. The proof of this fact was the main ingredient of Wiles' proof of Fermat's Theorem.

Theorem 4.1. *(Wiles–Taylor et al) Elliptic curves/$\mathbb{Q}$ are modular; in particular:*

- *$L(E, s)$ has an analytic continuation to $\mathbb{C}$,*
- *$L(E, s)$ satisfies the functional equation*

$$\widehat{L}(E, 2 - s) = w_{E/\mathbb{Q}} \cdot \widehat{L}(E, s)$$

where $\widehat{L}(E, s) := (\frac{\sqrt{N}}{2\pi})^s \cdot \Gamma(s)L(E, s)$ is ***the completed L-function*** *and $w_{E/\mathbb{Q}} = \pm 1$ is the* ***(global) root number*** (we'll return to this number later).

Conjecturally, the L-function encodes also the most important arithmetic properties of the elliptic curve:

Conjecture 4.2. *(Birch and Swinnerton-Dyer conjecture, BSD)*

$$\operatorname{ord}_{s=1} L(E, s) = \operatorname{rk} E/\mathbb{Q}$$

and the first non-zero Taylor coefficient of the L-function at $s = 1$ equals

$$\lim_{s\to 1} \frac{L(E, s)}{(s-1)^{\operatorname{rk} E/\mathbb{Q}}} = \frac{\#Ш(E)\Omega_E R_E \prod_{p|N} c_p}{(\#E(\mathbb{Q})_{tors})^2}$$

The quantities on the right hand side are arithmetic invariants of the curve; in particular $\#Ш(E)$ is the cardinality of **Shafarevich-Tate group** (which is not even known to be finite!). An easy consequence from BSD conjecture is

Conjecture 4.3. *(Parity conjecture)* $w_{E/\mathbb{Q}} = (-1)^{\mathrm{rk}\, E/\mathbb{Q}}$.

Today we know only that the BSD conjecture is true when the left side is ≤ 1 (as shown by Gross–Zagier–Kolyvagin). The parity conjecture is proven in a weaker form by Dokchitser–Dokchitser:

Theorem 4.4. *(Dokchitser - Dokchitser 2010, the p-Parity Theorem)*
For all elliptic curves $E/\mathbb{Q}$ and primes p: $w_{E/\mathbb{Q}} = (-1)^{\mathrm{rk}\, E/\mathbb{Q} + \mathrm{rk}_p(Ш(E)[p])}$.

Note that if the $Ш(E)$ group is finite, then $Ш(E)[p] = 0$ for sufficiently big p and the p-Parity Theorem implies the Parity Conjecture.
The root number is defined as a product of "local" root numbers:

$$w_{E/\mathbb{Q}} = \underbrace{w_{E/\mathbb{R}}}_{=-1} \cdot \prod_{p \in \mathbb{P}} w_{E/\mathbb{Q}_p}.$$

Analogously, for any other number field we take a product over all of its completions (with every infinite prime contributing -1). The formal definition of $w_{E/\mathbb{Q}_p}$ is complicated; however we have a following classification:

- if E has good reduction at p ($p \nmid \Delta_E$) then $w_{E/\mathbb{Q}_p} = 1$,
- if E has split multiplicative reduction at p ($p|\Delta_E$, $\widetilde{E} : y^2 = x^3 + \eta x$, $\eta \in \mathbb{F}_p^{\times 2}$) then $w_{E/\mathbb{Q}_p} = 1$,
- if E has non-split multiplicative reduction at p ($p|\Delta_E$, $\widetilde{E} : y^2 = x^3 + \eta x$, $\eta \notin \mathbb{F}_p^{\times 2}$), then $w_{E/\mathbb{Q}_p} = 1$,
- if E has additive reduction at p ($p|\Delta_E$, $\widetilde{E} : y^2 = x^3$) then $w_{E/\mathbb{Q}_p} = \pm 1$ *(it's possible to give a full classification, this was done by Halberstadt and there are $\approx$ 50 cases)*

Example 4.5. Let $E : y^2 + y = x^3 - x^2$. Then $\Delta_E = -11$, thus E has good reduction away from 11. It has split multiplicative reduction at 11, and so $w_{E/\mathbb{Q}} = (-1) \cdot (-1) = 1$.

Exercise 7. Let $K = \mathbb{Q}(\sqrt{17}, i)$. Prove, assuming the Parity Conjecture, that all elliptic curves defined over $\mathbb{Q}$ have even rank over K.

We have also the following

Conjecture 4.6. *(Root Number Equidistribution Conjecture)* 50% *of elliptic curves/$\mathbb{Q}$ have $w = 1$ and* 50% *have $w = -1$.*

It is equivalent to the following estimate:

$$\sum_{\substack{A,B \in \mathbb{Z} \\ H_{A,B} < x}} \mu(4A^3 + 27B^2) = o(x^{5/6}).$$

Bhargava and Shankar needed in their work a weaker result: curves with both root numbers have positive proportion.

Theorem 4.7. *(Bhargava – Shankar) Positive proportion of elliptic curves over $\mathbb{Q}$ have $w_{E/\mathbb{Q}} = 1$ and $w_{E/\mathbb{Q}} = -1$.*

Proof (sketch):
Let us for any curve $E : y^2 = x^3 + Ax + B$ denote: $E_{-1} : y^2 = x^3 + Ax - B$ (quadratic twist of E by -1). The proof conists of constructing a positive proportion family of elliptic curves $F \subset \mathcal{E}$ such that for any $E \in F$ we have $E_{-1} \in F$ and $w_{E/\mathbb{Q}} w_{E_{-1}/\mathbb{Q}} = -1$. Thus the root number is equidistributed in F, and since F has positive proportion (finer analysis allows to show that root number is equidistributed among at least 55% of curves.), the theorem follows. □

Another interesting problem is to analyse the distribution of the root number in various families of curves, like for example elliptic curves passing through the point $(0, 0)$. A conjecture of Goldfeld asserts for example that in the family of quadratic twists of a given curve the root number is equidistributed. The next conjecture justifies our interest in distribution of root number in families of curves.
Let's consider an elliptic curve $E/\mathbb{Q}(t)$ over function field in one variable (i.e. its coefficients are in fact rational functions in t). Then after substituting a number $a \in \mathbb{Q}$ in the place of t we obtain (in almost all cases) an "ordinary" elliptic curve $E_{t=a}/\mathbb{Q}$ (for example, if we take $E : ty^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ fixed, we obtain the "family of quadratic twists").

Conjecture 4.8. *(Minimalistic conjecture.) Let $E/\mathbb{Q}(t)$ be an elliptic curve of rank r. Then in the family $F = \{E_{t=a}\}$ for 100% of curves in F we have:*

$$\mathrm{rk}(E_{t=a}(\mathbb{Q})) = \begin{cases} r & \text{if } w(E_{t=a}) = (-1)^r \\ r+1 & \text{if } w(E_{t=a}) = (-1)^{r+1} \end{cases}$$

Note that this conjecture reveals the meaning of the root number – it controls the rank of a generic curve in a family.

5. Selmer groups

Definition 5.1. *(n-covering of a curve) A n-covering of an elliptic curve is a morphism $C \xrightarrow{\pi} E$ from any curve C of genus 1 such that $\pi = [n] \circ \varphi$ for some isomorphism $\varphi : C \xrightarrow{\simeq} E$ defined over $\overline{\mathbb{Q}}$ (here $[n]$ denotes the **multiplication–by–n map**: $[n]P = P + P + \ldots + P$).*
*The covering is **soluble** if $C(\mathbb{Q}) \neq \varnothing$.*
*The covering is **locally soluble** if $C(\mathbb{R}) \neq \varnothing$ and $C(\mathbb{Q}_p) \neq \varnothing$ for any prime p.*
*We call two n-coverings $(C, \pi = [n] \circ \varphi)$, $(C', \pi' = [n] \circ \varphi')$ **isomorphic**, if $\varphi'^{-1} \circ \varphi : C \to C'$ is defined over $\mathbb{Q}$.*

It turns out that the classes of isomorphisms of n-coverings are in 1-1 correspondence with the cohomology group $H^1(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, E[n])$, which allows us to introduce a group structure

in the set of n-coverings. The subgroup of soluble n-coverings corresponds to subgroup $E(\mathbb{Q})/nE(\mathbb{Q})$ of $H^1(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, E[n])$; the isomorphism is given by:

$$E(\mathbb{Q})/nE(\mathbb{Q}) \to \{ \text{ soluble } n\text{-coverings } \} \Big/ \sim$$

$$[P] \longmapsto \left(\begin{array}{c} n\text{-covering } \pi : E \to E \\ \pi(Q) = [n]Q + P \end{array} \right)$$

The locally soluble n-coverings form a subgroup called n^{th} **Selmer group** (denoted $\mathrm{Sel}_n E$). It's a finite abelian group with exponent n. In particular, for prime p we have $(\mathbb{Z}/p\mathbb{Z})^{s_p(E)}$ for some $s_p(E)$ called **p-Selmer rank**. Since $E(\mathbb{Q})/pE(\mathbb{Q}) \cong \frac{E(\mathbb{Q})_{tors}}{pE(\mathbb{Q})_{tors}} \oplus (\mathbb{Z}/p\mathbb{Z})^{\mathrm{rk}(E/\mathbb{Q})}$ injects into $\mathrm{Sel}_p(E)$ we have an inequality

$$\mathrm{rk}\, E/\mathbb{Q} \leq s_p(E)$$

The Selmer groups are in principle computable. They fit into an exact sequence:

$$1 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow \mathrm{Sel}_n E \longrightarrow Ш(E)[n] \longrightarrow 1$$

where $Ш(E)[n]$ denotes the n-torsion in the already mentioned **Tate–Shafarevich group**. Thus, this group measures the extent to which the Hasse principle fails to hold. Conjecturally, this group is finite, which gives us a chance of inventing an algorithm, that computes the rank of a given elliptic curve (note that then $Ш(E)[n] = 0$ for sufficiently large n and $E(\mathbb{Q})/nE(\mathbb{Q}) \cong Sel_n(E)$). However, at present, the Tate-Shararefich group remains one of the most mysterious groups in the number theory. It is known to be finite in the case when $\mathrm{ord}_{s=1} L(E, s) \leq 1$ (as shown by Gross – Zagier – Kolyvagin) and not in a single other case! We know also that the p-torsion parts of $Ш(E)$ can get arbitrarly large for $p = 2, 3, 5, 7$. However, a heuristics of Poonen and Rains predicts that the average size of Sel_n in $\mathcal{E}$ is $\sigma(n)$ (the sum of positive divisors of n) – in particular $1 + p$ when $n = p$ is a prime. Knowing the average size of Selmer group for a fixed n helps to bound the average rank of elliptic curves – to obtain their results, Bhargava and Shankar showed that heuristics of Poonen and Rains is correct for $n = 2, 3, 4, 5$.

In this four cases we are able to say something more about the n-coverings, using the following theorem:

Theorem 5.1. *(Swinnerton–Dyer–Cassels) Every soluble n-covering C of an ellitpic curve $E/\mathbb{Q}$ has a divisor $D \in \mathrm{Div}^n(C)$ defined over $\mathbb{Q}$.*

This theorem enables us (analogously as in theorem 3.1) to obtain an explicit embedding $C \xrightarrow{|D|} \mathbb{P}^{n-1}$ defined over $\mathbb{Q}$ into projective space for $n \in \{2, 3, 4, 5\}$:

- $n = 2$: $C \longrightarrow \mathbb{P}^1$ is a double cover, and realizes C a binary quartic curve:

$$y^2 = ax^4 + bx^3y + \ldots + ey^4, \qquad a, \ldots, e \in \mathbb{Q}$$

- $n = 3$: $C \hookrightarrow \mathbb{P}^2$, image of C is given by a ternary cubic $ax^3 + bx^2y + \ldots + jz^3 = 0$
- $n = 4$: $C \hookrightarrow \mathbb{P}^3$, image of C is an intersection of two quartics,
- $n = 5$: $C \hookrightarrow \mathbb{P}^4$, image of C is defined by a degree 5 polynomial.

We will concentrate on two cases:

(A) $n = 2$ – we have a correspondence:

$$\left\{ \begin{array}{c} \text{2–Selmer elements} \\ \text{of elliptic curves} \end{array} \right\} \quad \overset{1-1}{\longleftrightarrow} \quad \left\{ \begin{array}{c} \text{locally soluble} \\ \text{binary quartics} \end{array} \right\} \Big/ \, \mathrm{Gl}_2(\mathbb{Q})\text{–equivalence}$$

(B) $n = 3$ – we have a correspondence:

$$\left\{ \begin{array}{c} \text{3–Selmer elements} \\ \text{of elliptic curves} \end{array} \right\} \quad \overset{1-1}{\longleftrightarrow} \quad \left\{ \begin{array}{c} \text{locally soluble} \\ \text{ternary cubics} \end{array} \right\} \Big/ \, \mathrm{Gl}_3(\mathbb{Q})\text{–equivalence}$$

6. Composition of forms

The idea of composing forms comes from Gauss, who introduced composition of binary quadratic forms in his *Disquisitiones Arithmeticae*.
Let us denote by $V = \{f(x, y) = ax^2 + bxy + cy^2 : a, b, c \in \mathbb{Z}\}$ the set of binary quadratic forms. We summarise briefly the main results concerning binary quadratic forms:

- $\mathrm{Sl}_2(\mathbb{Z})$ acts on V – matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ takes $f(x, y)$ to $f(\alpha x + \beta y, \gamma x + \delta y)$,

- there is a unique polynomial $\mathrm{Sl}_2(\mathbb{Z})$–invariant ("discriminant") given by $D_f = b^2 - 4ac$, that generates the invariant ring: $\mathbb{Z}[a, b, c]^{\mathrm{Sl}_2(\mathbb{Z})} = \mathbb{Z}[b^2 - 4ac]$.

- number D is a discriminant of a form from V if and only if it satisfies the congruence condition $D \equiv 0, 1 \pmod 4$,

- the set $H_D = \{f \in V : D_f = D\}/(\mathrm{Sl}_2(\mathbb{Z}) - \textit{equivalence})$ of orbits of $\mathrm{Sl}_2(\mathbb{Z})$–action on quadratic forms with given discriminant is finite – its size is denoted by h_D; it can be identified with a narrow class group of a unique quadratic order of discriminant D, namely $R_D = \mathbb{Z} + n\mathcal{O}_{\mathbb{Q}(\sqrt{D_0})}$ (where $D = n^2 D_0$ and D_0 is a fundamental discriminant); thus we can compose forms by transferring the group law.

- we have following asympthotic formulas for negative and positive discriminants (conjectured by Gauss and proven by Siegel and Mertens respectively):

  $$\sum_{-x<D<0} h_D \sim \frac{\pi}{18\zeta(3)} x^{3/2}, \qquad \sum_{0<D<x} h_D \log \varepsilon_D \sim \frac{\pi^2}{18\zeta(3)} x^{3/2}, \qquad \text{for } x \to \infty$$

  where ε_D denotes the fundamental unit of R_D.

Gauss' idea can be generalized for example in the case of binary cubic forms. Analogously we introduce action of $\mathrm{Gl}_2(\mathbb{Z})$ on $V = \{f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 : a,b,c,d \in \mathbb{Z}\}$ and a discriminant D_f. The set of $\mathrm{Gl}_2(\mathbb{Z})$-equivalence classes of forms with given discriminant D is finite and can be identified with orders of discriminant D in cubic fields. Moreover, as shown by Davenport, we have asympthotic formulas:

$$\sum_{-x<D<0} h_D \sim \frac{\pi^2}{24}x \qquad \text{and} \qquad \sum_{0<D<x} h_D \sim \frac{\pi^2}{72}x \qquad \text{for } x \to \infty$$

In his PhD thesis, Manjul Bhargava studies 10 more situations when there is a space of forms (or objects closely related to forms) with one polynomial invariant, the discriminant, and introduces a group structure analogous to Gauss' composition law. Recently, Bhargava and Shankar have developed a machinery to analyze and count orbits on 'coregular spaces' with more than one invariant. ('Coregular' simply means that the invariant ring is a polynomial ring in finitely many basic invariants.) Two of these cover the cases that we want to discuss:

(A) $V = \{f(x,y) = ax^4 + bx^3y + \ldots + ey^4 : a,\ldots,e \in \mathbb{Z}\}$ – binary quartic forms with action of $G = \mathrm{Gl}_2(\mathbb{Z})$,

(B) $V = \{f(x,y,z) = ax^3 + \ldots + jz^3 : a,\ldots,j \in \mathbb{Z}\}$ – ternary cubic forms with action of $G = \mathrm{Sl}_3(\mathbb{Z})$.

Both cases can be treated similarly – there exist two G-invariants $I = I_f$, $J = J_f$ (some specific polynomials in the coefficients of f, defined separately for case **(A)** and **(B)**), such that the ring of G–invariants is freely generated by I, J. Agan, integers $I, J \in \mathbb{Z}$ are invariants of some form iff they satisfy certain congruence conditions. We define the discriminant of a form to be $\Delta_f := \frac{4I^3 - J^2}{27}$ and the height of a form: $H_f = H_{I,J} = \max\{|I|^3, \frac{1}{4}|J|^2\}$.

Let us look at Case **(B).** As before, it is possible to estimate the number of desired ternary cubic forms with given invariants (an analogous theorem holds also for binary quartic forms):

Theorem 6.1. *(Bhargava–Shankar) Let $h_{I,J}$ be the number of strongly irreducible ternary cubic forms with invariants I, J, up to equivalence. Then*

$$\sum_{I,J:H_{I,J}<x} h_{I,J} = \frac{32}{45}\zeta(2)\zeta(3)x^{5/6} + o(x^{5/6}), \qquad \textit{for } x \to \infty$$

(note that the sum on the left hand side has approximately $\frac{32}{45}x^{5/6}$ terms, so that we get that on average h_{IJ} equals $\zeta(2)\zeta(3)$) and

$$\sum_{\substack{I,J:H_{I,J},\\ \Delta<0}} h_{I,J} = \frac{128}{45}\zeta(2)\zeta(3)x^{5/6} + o(x^{5/6}), \qquad \textit{for } x \to \infty$$

This theorem applies also to forms in any congruence family of forms.

Proof (overview):
In order to count the eligible forms, we parametrize them as the orbits of an algebraic group acting on a real vector space. Then we consider the fundamental domain for the group action and approximate the number of lattice points inside of it by its volume (using methods from Minkowski's geometry of numbers). The hardest part is dealing with cusps inside the fundamental domain, however it turns out that they mostly contain reducible forms. □

This result can be applied to find the average cardinality of Selmer groups:

Theorem 6.2. *(Bhargava–Shankar)*
The average cardinality of $\mathrm{Sel}_n(E)$ *for* $n \in \{2, 3, 4, 5\}$ *is* $\sigma(n)$.

Proof (overview):
We present the main steps of Bhargava–Shankar's proof for $n = 3$:

1) we have a one-to-one correspondence between the sets

$$\left\{\begin{array}{c}\mathrm{PGl}_3(\mathbb{Q})\text{-orbits of strongly irreducible}\\ \text{locally soluble ternary cubic forms with}\\ \text{rational coefficients and invariants}\\ I_f = -3A, J_f = -27B\end{array}\right\} \overset{1-1}{\longleftrightarrow} \left\{\text{nontrivial elements of } \mathrm{Sel}_3(E_{A,B})\right\}$$

– any ternary cubic form f yields a curve $C : f = 0$ from the Selmer group.

2) the results of Cremona–Fisher–Stoll concerning $\mathbb{Z}$-models for genus 1 curves allow to minimise and reduce the Selmer elements, by replacing $\mathbb{Q}$-coefficients by $\mathbb{Z}$-coefficients and $\mathrm{PGl}_3(\mathbb{Q})$–orbits by $\mathrm{PGl}_3(\mathbb{Q})$–equivalence classes.

3) each $\mathrm{PGl}_3(\mathbb{Q})$–orbit is a finite sum of $\mathrm{Sl}_3(\mathbb{Z})$ orbits. After introducing a proper "weight" (equal to $\frac{1}{\#\text{ orbits}}$) we can count $\mathrm{Sl}_3(\mathbb{Z})$–orbits.

4) Count the orbits using Theorem 6.1.

5) Sieving allows infinitely many congruence conditions to get the result for locally soluble forms.

□

7. Average rank

In this section we'll show how to obtain bounds on average rank knowing the average cardinality of Selmer groups. Denote by avg and $\overline{\text{avg}}$ the average and upper average respectively. Let's suppose for a moment that the Poonen–Rains heuristics works for infinitely many

p, i.e. $\operatorname{avg} \#Sel_p(E) = 1 + p$. Then combining the inequalities: $\operatorname{rk} E/\mathbb{Q} \leq s_p(E)$ and $(p^2 - p)k + 2p - p^2 \leq p^k$ (valid for $k = 0, 1, 2, \ldots$):

$$(p^2 - p) \operatorname{rk} E/\mathbb{Q} + 2p - p^2 \leq (p^2 - p)s_p(E) + 2p - p^2 \leq p^{s_p(E)} = \# \operatorname{Sel}_p(E)$$

By substituting $\operatorname{avg} \operatorname{Sel}_p = 1 + p$ we get:

$$\overline{\operatorname{avg}} \operatorname{rk} E/\mathbb{Q} \leq 1 + \frac{1}{p^2 - p}$$

– thus with $p \to \infty$ we would get the bound $\overline{\operatorname{avg}} \operatorname{rk} E(\mathbb{Q}) \leq 1$. This shows, that in order to show that the average rank is $\leq \frac{1}{2}$, we need some additional input. It comes from the parity of the rank:

Proposition 7.1. *If* $\operatorname{avg} \operatorname{Sel}_p(E) = 1+p$ *for infinitely many primes* p *and the* ***Root Number Equidistribution Conjecture*** *4.6 holds, then* $\overline{\operatorname{avg}} \operatorname{rk} E/\mathbb{Q} \leq \frac{1}{2}$ *and elliptic curves of rank 0 have density* $\geq \frac{1}{2}$*. If we assume moreover the* ***Parity Conjecture*** *4.3 then* $\overline{\operatorname{avg}} \operatorname{rk} E/\mathbb{Q} = \frac{1}{2}$ *and elliptic curves of rank zero and one each have density* $\frac{1}{2}$*.*

Proof (sketch):
We need to consider odd and even rank separately, using the inequalities:

$\frac{p^2-1}{2} \cdot k + 1 \leq p^k$ for even k,
$\frac{p^3-p}{2} \cdot k + \frac{3p-p^3}{2} \leq p^k$ for odd k.

Using p-Parity Theorem and Root Number Equidistribution we obtain the inequality $\overline{\operatorname{avg}} \operatorname{rk} E/\mathbb{Q} \leq \frac{1}{2}\frac{p+1}{p-1}$ and by taking $p \to \infty$: $\overline{\operatorname{avg}} \operatorname{rk} E/\mathbb{Q} \leq \frac{1}{2}$. □

The final argument in Bhargava–Shankar's proof that the average rank of elliptic curves over $\mathbb{Q}$ is less than 1 is similar to the above reasoning. They use the result $\operatorname{avg} \operatorname{Sel}_5(E) = 6$, the p-parity theorem and the fact that the Equidistribution Root Number Conjecture holds for 55% of curves (4.7) to get average rank below 1 (approximately 0.885). They also deduce that positive proportion of elliptic curves over $\mathbb{Q}$ satisfies BSD conjecture by using Skinner-Urban Theorem (which can be roughly restated like this: if p is an odd prime, $s_p(E) = 0$ and E satisfies some technical conditions, then $L(E, 1) \neq 0$) and the result of Gross–Zagier–Kolyvagin. Currently Bhargava and Shankar are working on analogous results for hyperelliptic curves.

Hints for the exercises

Exercise 1. Let $P_0 \in C(\mathbb{Q})$. Parametrize other points in $C(\mathbb{Q})$ by considering all lines through P_0 with rational slopes and their intersections with C.

Exercise 2. Show that $x^2 + y^2 = 3$ has no solutions in $\mathbb{Q}_3$; in other words show that if $X^2 + Y^2 = 3Z^2$ for $X, Y, Z \in \mathbb{Z}$ then $3|X, Y, Z$.

Exercise 3. Note that $\{\mathcal{O}, (-1,0), (0,\pm 1), (2,\pm 3)\} \subset E(\mathbb{Q})_{tors}$. We have: $\#\widetilde{E}(\mathbb{F}_5) = 6$ – thus 3.4 and **Lagrange theorem** imply $\#E(\mathbb{Q})_{tors}|6$.

Exercise 4. The injection $E_d(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}(\sqrt{d}))$ is $\iota((x,y)) = (x, \sqrt{d}y)$. Show that: $\iota(E_d(\mathbb{Q})) \cap E(\mathbb{Q}) \subset E(\mathbb{Q})[2]$ and $2E(\mathbb{Q}) \subset \iota(E_d(\mathbb{Q})) + E(\mathbb{Q})$ to obtain the equality of ranks.

Exercise 5. If you view $E(K) \otimes \mathbb{C}$ as a representation of $G = Gal(K/\mathbb{Q})$, it decomposes into irreducible complex representations of G. The rank of $E(\mathbb{Q})$ is equal to number of trivial representations in this decomposition. Prove that every group of odd order has only one irreducible representation which is real, namely the trivial one, and the rest come in complex-conjugate pairs (note that in every group the number of self-inverse conjugacy classes equals the number of real irreducible representations). Alternatively, use the Feit-Thompson theorem.

Exercise 6. Use Vieta's formulas to show that if $x^3 + Ax + B$ has integer roots then A and B must be "large".

Exercise 7. This is a question about how primes split in $\mathbb{Q}(\sqrt{17}, i)$. Use the definition of the global root number as a product of local root numbers.