ARITHMETIC STATISTICS

HYUN JONG KIM

September 13, 2025

Contents

The purpose of this document is to formulate and discuss conjectures (both unproven and proven) in arithmetic statistics.

1. Conjectures and heuristics on elliptic Curves and abelian varieties over function fields

1.1. Sato-Tate distribution of traces of Frobenii of elliptic curves over number fields.

Clozel, Harris, Shepherd-Barron, and Taylor [CHT08], [Tay08], [HSBT05] first proved the Sato-Tate conjecture for non CM elliptic curves over totally real fields under mild hypotheses (that the elliptic curve has at least one prime of multiplicative reduction). The mild hypotheses were removed in by Barnet-Lamb, Geraghty, Harris, and Taylor [BLGHT11]. loc. cit. in fact proved the natural generalization of the Sato-Tate conjecture for regular algebraic cuspidal automorphic rperesentations of $\mathrm{GL}_2(\mathbb{A}_F)$ where F is a totally real field which are not of CM type.

Theorem 1.1.1 (Sato-Tate theorem for non-CM elliptic curves over totally real fields)**.** (♠ TODO: define elliptic curve, CM) (♠ TODO: define trace of Frobenius, reduction of elliptic curve) Let F be a totally real number field and E/F be an elliptic curve without complex multiplication (CM). For each prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ where E has good reduction, define the angle $\theta_{\mathfrak{p}} \in [0,\pi]$ by

$$\theta_{\mathfrak{p}} = \cos^{-1}\left(\frac{a_{\mathfrak{p}}}{2\sqrt{N\mathfrak{p}}}\right),$$

where $a_{\mathfrak{p}}$ is the trace of Frobenius at $\mathfrak{p}$ and $N\mathfrak{p}$ is the norm of $\mathfrak{p}$.

Then for every interval $[\alpha,\beta] \subseteq [0,\pi]$, we have

$$\lim_{X\to\infty} \frac{\#\{\mathfrak{p} : N\mathfrak{p} \le X, \alpha \le \theta_{\mathfrak{p}} \le \beta\}}{\#\{\mathfrak{p} : N\mathfrak{p} \le X\}} = \frac{2}{\pi}\int_{\alpha}^{\beta} \sin^2\theta\, d\theta = \frac{1}{\pi}\big(\beta - \alpha + \sin\alpha\cos\alpha - \sin\beta\cos\beta\big).$$

Intuitively, the Sato-Tate conjecture states that $\frac{a_{\mathfrak{p}}}{2\sqrt{N\mathfrak{p}}}$ is equidistributed in $[-1,1]$ with respect to the measure $\frac{2}{\pi}\sqrt{1-t^2}dt$ or equivalently that $\theta_{\mathfrak{p}}$ is equidistributed in $[0,\pi]$ with respect to the measure $\frac{2}{\pi}\sin^2\theta d\theta$.

1.2. Mordell-Weil Ranks of abelian varieties over global fields and their Selmer groups.

1.2.1. *Minimalist conjecture for Mordell-Weil ranks of elliptic curves over global fields.*

Theorem 1.2.1 (Mordell–Weil Theorem)**.** (♠ TODO: for function fields, I think I need to say that the curve is not isotypical) (♠ TODO: Try to find a mordell-weil statement over $\mathbb{Q}(T)$) Let K be a global field (Definition C.0.1), and let E be an abelian variety (Definition C.0.2) defined over K. Then the group $E(K)$ of K-rational points on E is a

finitely generated abelian group; that is, there exist integers $r \geq 0$ and a finite abelian group T such that

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

Here, r is called the *Mordell–Weil rank of E over K* or the *algebraic rank of E over K*, and T is the torsion subgroup of $E(K)$.

In 1979, Goldfeld [Gol06] first conjectured that elliptic curves over $\mathbb{Q}$, when arranged in a suitable manner, should be $\frac{1}{2}$ on average. Katz and Sarnak [KS99] gave a refined statistical model for understanding average and typical Mordell-Weil ranks of elliptic curves — they conjectured that as the conductor of the elliptic curves grows large, the distribution of zeroes of their L-functions "statistically behaves like" eigenvalues of random matrices from classical compact groups (e.g. unitary, symplectic, or orthogonal groups). The generally held conjecture for more general elliptic curves over number fields is that asymptotically 50% of such elliptic curves should be of Mordell-Weil rank 0, asymptotically 50% of such elliptic curves should be of Mordell-Weil rank 1, and asymptotically 0% of such elliptic curves curves should be of Mordell-Weil rank ≥ 2.

Conjecture 1.2.2 (Minimalist Conjecture for Mordell–Weil ranks of elliptic curves over global fields)**.** Let E be an elliptic curve (Definition A.0.1) defined over a global field (Definition C.0.1) K. Denote by $r(E/K)$ the Mordell–Weil rank (Theorem 1.2.1) of $E(K)$, i.e., the rank of the finitely generated abelian group $E(K)$. (♠ TODO: discuss some such stuiable families; e.g. height vs. conductor)

The *Minimalist Conjecture* predicts that as E varies over suitable families of elliptic curves defined over K, ordered in some appropriate manner, the distribution of the Mordell–Weil ranks is minimal in the sense that:

- The probability that $r(E/K) = 0$ is 50%.
- The probability that $r(E/K) = 1$ is 50%.
- The probability that $r(E/K) \geq 2$ tends to 0.

In particular, almost all elliptic curves over K are expected to have Mordell–Weil rank either 0 or 1.

(♠ TODO: discuss function field case, etc.)

Bhargava and Shankar proved that the average rank of elliptic curves over $\mathbb{Q}$ is bounded above, first by $\frac{3}{2}$ [BS15a] and later by $\frac{7}{6}$ [BS15b] by computing the average size of the 2-Selmer and the 3-Selmer groups (Definition D.0.1) of elliptic curves $E/\mathbb{Q}$ respectively. Their results assume neither the Birch-Swinnerton-Dyer conjecture nor the Generalized Riemann hypothesis, both of which were assumed in previous works of A. Brumer [Arm92], Heath-Brown [HB04], and Young [You06], which respectively obtained upper bounds of 2.3, 2, and $\frac{25}{14}$.

Baig and Hall [BH12] computed empirical evidence to support the minimalist conjecture for elliptic curves over function fields, albeit the proportion of curves of rank 1 and of rank 2 seem to converge to the respective predicted values of 50% and 0% rather slowly.

1.2.2. *Poonen-Rains [PR] and Bhargava-Kane-Lenstra-Poonen-Rains [BKLPR].* See [Poo18] for Bjorn Poonen's introduction to this topic, submitted to the 2018 ICM Proceedings.

Conjecture 1.2.3 (Poonen-Rains conjecture [PR12, Conjecture 1.1])**.** Let K be a global field (Definition C.0.1) and let ℓ be a prime number. Below, averages/probabilities are taken over elliptic curves "ordered by" some reasonable notion of height; the statistics are defined by considering the finitely many elliptic curves of height $\leq B$, and take the limit of the statistics as $B \to \infty$. A standard reasonable height for elliptic curves over number fields would be the naive height (Definition E.0.1)

1. ([PR12, Conjecture 1.1(a)]) As E varies over all elliptic curves over K
$$\mathrm{Prob}(\dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell E = d) = \left(\prod_{j\geq 0}(1+p^{-j})^{-1}\right)\cdot\left(\prod_{j=1}^{d}\frac{p}{p^j-1}\right).$$
(in particular,)
2. ([PR12, Conjecture 1.1(b),(c)], cf. [Poo18, Conjecture 3.4]) For $m \in \mathbb{Z}_{\geq 0}$,
$$\mathrm{Average}_{E/K}\left((\#\,\mathrm{Sel}_\ell E)^m\right) = \prod_{i=1}^{m}(\ell^i+1),$$
i.e. the average of $(\#\,\mathrm{Sel}_p E)^m$ over all E/K is $\prod_{i=1}^{m}(\ell^i+1)$. In particular, the average of $\#\,\mathrm{Sel}_\ell E$ over all E/K is $\ell+1$; consequently, the average of $\#\,\mathrm{Sel}_n E$ over all E/K, where $n \geq 1$, is $\sigma(n)$.

Under the assumption that the parity of the Mordell-Weil rank (Theorem 1.2.1) is equidistributed over E/K, these recover the minimalist conjecture

Definition 1.2.4. [cf. [FLR23, 1.2.1]] (♠ TODO: define minimal weierstrass model, and state this as a concept) Let $\mathbb{F}_q$ be a finite field of odd characteristic. Any elliptic curve (Definition A.0.1) $E/\mathbb{F}_q(t)$ has a minimal Weierstrass model of the form
$$y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$$
where $a_i(t)$ is a polynomial of degree $2id$ for $i \in \{1,2,3\}$. The *height of E*, which may be denoted by $h(E)$, is defined to be rhe value of d, which is uniquely determined by E.

Definition 1.2.5. Let $\mathbb{F}_q$ be a finite field of odd characteristic and let $n \geq 2$.

1. (cf. [FLR23, 1.2.1, Definition 1.3]) Let $(\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q}$ be the joint probability distribution on $\mathbb{Z}_{\geq 0} \times \mathrm{Ab}_n$, where Ab_n is the set of isomorphism classes of finite $\mathbb{Z}/n\mathbb{Z}$-modules, assigning to a pair $(r, G) \in \mathbb{Z}_{\geq 0} \times \mathrm{Ab}_n$ the proportion of isomorphism classes of height (Definition 1.2.4) d elliptic curves over $\mathbb{F}_q(t)$ with Mordell-Weil rank (Theorem 1.2.1) and n-Selmer group (Definition D.0.1) isomorphic to G. More precisely,
$$\mathrm{Prob}((\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q} = (r, G)) = \frac{\#\{E/\mathbb{F}_q(t) : h(E) = d, \mathrm{rk}(E) = r, \mathrm{Sel}_n(E) \simeq G\}}{\#\{E/\mathbb{F}_q(t) : h(E) = d\}}.$$

2. (cf. [FLR23, Definition 5.12]) Let $(\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}})$ be the joint distribution on $\mathbb{Z}_{\geq 0} \times \mathrm{Ab}_n$ defined by

$$\mathrm{Prob}((\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}}) = (r, G)) = \begin{cases} \frac{1}{2}\mathscr{T}_{r,\mathbb{Z}/n\mathbb{Z}} & \text{if } r \leq 1 \\ 0 & \text{if } r \geq 2 \end{cases}$$

(♠ TODO: define $\mathscr{T}_{r,\mathbb{Z}/n\mathbb{Z}}$)

[PR12]

[FLR23] roughly proved that the rank and Selmer groups amongst elliptic curves $E/\mathbb{F}_q(t)$ of height d in the $\lim_{d\to\infty}\lim_{q\to\infty}$ limit are distributed according to the BKLPR heuristic:

Theorem 1.2.6 ([FLR23, Theorem 1.1])**.** (♠ TODO: state) Let $n \geq 1$ be a fixed integer. The limits

$$\lim_{d\to\infty} \limsup_{\substack{q\to\infty \\ \gcd(q,2n)=1}} (\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q} \quad \text{and} \quad \lim_{d\to\infty} \liminf_{\substack{q\to\infty \\ \gcd(q,2n)=1}} (\mathrm{rk}, \mathrm{Sel}_n)^d_{\mathbb{F}_q},$$

Definition 1.2.5 where q ranges over prime powers, exist, are equal to each other, and coincide with the distribution $(\mathrm{rk}^{\mathrm{BKLPR}}, \mathrm{Sel}_n^{\mathrm{BKLPR}})$ predicted by the BKLPR heuristic (Definition 1.2.5). More precisely,

1.2.3. *Parity conjecture on the parity of the Mordell-Weil rank of an elliptic curve over a global field and on the root number associated to its L-function.*

1.2.4. *Goldfeld's conjecture on the ranks in families of quadratic twists of elliptic curves over global fields.*

1.2.5. *Conjectures on the boundedness on the Mordell-Weil ranks of abelian varieties over global fields.* (♠ TODO: add Alexnader smith's results over number fields)

1.3. **Analytic ranks of abelian varieties over global fields.**

1.3.1. *The Birch-Swinnerton-Dyer conjecture.* The Birch and Swinnerton-Dyer conjecture (often abbreviated as the BSD conjecture), relates the Mordell-Weil rank (Theorem 1.2.1) of elliptic curves with their analytic rank.

(♠ TODO: define trace of frobenius)

The conjecture was originally formulated in terms of asymptotics of the traces of Frobenii:

Conjecture 1.3.1 (Original Birch-Swinnerton-Dyer conjecture [BSD65])**.** (♠ TODO: define the discriminant of an elliptic curve, reduction type) Let $E/\mathbb{Q}$ be an elliptic curve and let Δ be its discriminant. For a prime p of good reduction, we have

$$\prod_{p\leq X} \frac{a_p}{p} \approx C \log(X)^r \quad \text{as} \quad X \to \infty$$

where r is the Mordell-Weil rank of $E/\mathbb{Q}$ (Theorem 1.2.1) and where C is some constant depending on E.

(♠ TODO: define the hasse-weil L-function) The modern formulation of the conjecture is expressed in terms of the Hasse-Weil L-function $L(E, s)$. In fact, it can be stated for abelian varieties over number fields:

Conjecture 1.3.2 ([Tat66], cf. [Jor05])**.** Let A/K be an abelian variety (Definition C.0.2) over a number field (Definition C.0.1). Write $L(A, s)$ for the Hasse-Weil L-function of A.

1. (*weak BSD conjecture*; [Tat66, (A)]) The order of vanishing of L at 1 equals the Mordell-Weil rank of A (Theorem 1.2.1). (♠ TODO: define regulartor, shafarevich-tate group, and a statement that Sha is finite)
2. (*strong BSD conjecture*; [Tat66, (B)], cf. [Jor05, Conjecture 3.15]) Let $A(K)_{\text{tors}}$ and $A^\vee(K)_{\text{tors}}$ be the torsion subgroups of $A(K)$ and $A^\vee(K)$ respectively. Let R_A be the regulator of A, and let $Ш(A/K)$ be the Shafarevich-Tate group, which is finite. We have
$$\frac{L^{(r)}(A,1)}{r!\int_{A(\mathbb{A}_K)} d\mu_{A,w,\Lambda}} = \frac{R_A|Ш(A/K)|}{|A(K)_{\text{tors}}|\cdot|A^\vee(K)_{\text{tors}}|}.$$
(♠ TODO: define the measure used in the integral) It may be of interest from the computational perspective to rewrite the above equation in the form
$$\frac{1}{r!}L^{(r)}(A,1) = \frac{P_A\cdot R_A\cdot|Ш(A/K)|\cdot\prod_{v\in M_K^0} c_v}{\sqrt{|D_K|}^d\cdot|A(K)_{\text{tors}}|\cdot|A^\vee(K)_{\text{tors}}|}$$
where (♠ TODO: define period, tamagawa number, absolute discriminant)
   - P_A is the the period of A
   - M_K^0 is the collection of finite places of K
   - c_v is the Tamagawa number at the finite place $v \in M_K^0$
   - D_K is the absolute discriminant of K

The original BSD conjecture (Conjecture 1.3.1) is equivalent to the weak BSD conjecture (Conjecture 1.3.2) for elliptic curves over number fields.

(♠ TODO: see if there is a function field analogue of BSD)

The weak and strong BSD conjectures can be formulated over function fields as well. In this case, Tate's conjecture (Conjecture B.0.1) for elliptic surfaces is equivalent to weak BSD for elliptic curves over the generic fibers.

(♠ TODO: cite the original source of this theorem; it should be either Tate or Grothendieck, see Caleb Ji's notes on the tate conjecture)

Theorem 1.3.3. Let $K = \mathbb{F}_q(C)$ be the function field of a smooth projective curve C over $\mathbb{F}_q$. Let E/K be an ellpitic curve. Let $\mathcal{E}$ be the unique elliptic surface(♠ TODO: define elliptic surface) over $\mathbb{F}_q$ with generic fiber E. (♠ TODO: define generic fiber) The following are equivalent:

1. Tate's conjecture (Conjecture B.0.1) for the smooth projective variety $\mathcal{E}/\mathbb{F}_q$
2. The weak BSD conjecture for the elliptic curve E/K.

1.3.2. *Nagao's conjecture.* (♠ TODO: how well does this discussion hold for elliptic surfaces over number fields?)

Definition 1.3.4. (♠ TODO: define a non-split elliptic surface) Let $\mathcal{E} \to \mathbb{P}^1$ be a non-split elliptic surface over $\mathbb{Q}$ with Weierstrass equation (Definition A.0.2)

$$\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$$

with $4A(T)^3 + 27B(T)^2 \neq 0$; take $A(T), B(T) \in \mathbb{Z}[T]$. For $t \in \mathbb{Z}$, let E_t be the specialization of $\mathcal{E}$ obtained by letting $T = t$; for all but finitely many integers t, in fact for the t at which the j-invariant (Definition A.0.4) $j(\mathcal{E}) \in \mathbb{Q}(T)$ is defined and nonvanishing, E_t is an elliptic curve over $\mathbb{Q}$. Further let $E_{t,p}$ denote the reduction of $E_t/\mathbb{Q}$ at the prime p. (♠ TODO: define reduction) Write

$$A_p(\mathcal{E}) = \frac{1}{p}\sum_{t=0}^{p-1} a_p(E_t)$$

where $a_p(E_t)$ is the usual trace of Frobenius of E_t at p (♠ TODO: define the trace of Frobenius at a prime, taking reduction into consideration) and

$$S(N, \mathcal{E}) = -\frac{1}{N}\sum_{p \text{ prime} \leq N} A_p(\mathcal{E}) \cdot \log p$$

One might refer to $S(N, \mathcal{E})$ as a *Nagao sum for* $\mathcal{E}$.

(♠ TODO: define Mestre-Nagao sum)

Conjecture 1.3.5 (Nagao's conjecture [Nag97])**.** Let $\mathcal{E} \to \mathbb{P}^1$ be a non-split elliptic surface over $\mathbb{Q}$. The value $S(N, \mathcal{E})$ (Definition 1.3.4) converges as $N \to \infty$ and converges to the Mordell-Weil $\mathbb{Q}(T)$-rank of $\mathcal{E}$ (♠ TODO: define the $\mathbb{Q}(T)$-rank of an elliptic surface).

Rosen and Silverman proved that Nagao's conjecture for elliptic surface $\mathcal{E}$ over $\mathbb{Q}$ assuming that Tate's conjecture holds for $\mathcal{E}$:

Theorem 1.3.6 ([RS98, Theorem 1.3])**.** (♠ TODO: state Nagao's conjecture in terms of elliptic surfaces over number fields; Rosen and Silverman's theorem is about that context in general.)

S. Kim and M. Ram Murty[KM23] proved the following about the Nagao-Mestre sum. See [KM23, Section 4] for a discussion that relates their results to Nagao's conjecture (Conjecture 1.3.5).

Theorem 1.3.7 ([KM23])**.** Let $E/\mathbb{Q}$ be an elliptic curve (Definition A.0.1) with discriminant Δ_E. For each prime p of good reduction, i.e. $p \nmid \Delta_E$, (♠ TODO: define reduction) let a_p be the trace of Frobenius. Let a_p be 0, 1, or -1 if E has additive, split multiplicative, and nonsplit multiplicative reductive at p respectively.

If the limit

$$\lim_{X \to \infty} \frac{1}{\log X} \sum_{p < X} \frac{a_p \log p}{p}$$

exists, then (♠ TODO: describe the riemann hypothesis for L_E)

1. ([KM23, Corollary 7]) the Riemann hypothesis for $L_E(s)$ is true, and the limit is $-r+\frac{1}{2}$, and
2. ([KM23, Corollary 8]) the original BSD conjecture (Conjecture 1.3.1) is true for the elliptic curve $E/\mathbb{Q}$.

1.4. **Selmer groups and their distributions.**

1.5. **Modularity conjecture.**

2. Hasse-Weil conjecture on the behavior of Hasse-Weil L-functions on varities over global fields

3. Random matrices

4. Catalan's conjcture

5. Conjectures on distributions/counts of number fields and function fields

5.1. **Malle's conjecture.**

5.2. **Cohen-Lenstra heuristics.**

Appendix A. Elliptic curves

Definition A.0.1 (Elliptic curve over a scheme)**.** Let S be a scheme. An *elliptic curve over S* is a pair (E, π) where

- E is a scheme together with a morphism $\pi : E \to S$,
- (E, π) is an abelian scheme of relative dimension 1 over S, i.e. π is proper, smooth, of relative dimension 1, with geometrically connected fibers, and
- a chosen section $e : S \to E$, called the *zero section*, endowing (E, π) with the structure of a commutative group scheme over S.

Equivalently, an elliptic curve over S is a smooth proper curve of genus 1 over S together with a marked S-point that plays the role of the identity.

Definition A.0.2 (General Weierstrass Equation over a Ring)**.** (♠ TODO: define homogenization of a polynomial) Let R be a (commutative unital) ring, and let $a_1, a_2, a_3, a_4, a_6 \in R$.

A *general Weierstrass equation over R* is either of the following equivalent descriptions:

- The affine equation in variables x, y over R

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

- The projective cubic equation
$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$
in homogeneous coordinates X, Y, Z. Note that this defines a closed subscheme inside $\mathbf{P}^2_R = \operatorname{Proj} R[X, Y, Z]$.

A *short Weierstrass equation over R* is a Weierstrass equation for which $a_1 = a_3 = a_2 = 0$, having the form
$$y^2 = x^3 + a_4x + a_6,$$
or equivalently one which has projective homogenization
$$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3.$$

Notation A.0.3 (Auxiliary Invariants for a General Weierstrass Equation)**.** Let R be a (commutative unital) ring. For the general Weierstrass equation
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$
with coefficients $a_1, a_2, a_3, a_4, a_6 \in R$, the following are standard notation:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= 2a_4 + a_1a_3, \\
b_6 &= a_3^2 + 4a_6, \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6
\end{aligned}$$

For a short Weierstrass equation (Definition A.0.2)
$$y^2 = x^3 + Ax + B,$$
with $A, B \in R$, these invariants simplify as follows:

$$\begin{aligned}
b_2 &= 0, \\
b_4 &= 2A, \\
b_6 &= 4B, \\
b_8 &= -A^2, \\
c_4 &= -24b_4 = -48A, \\
c_6 &= -216b_6 = -864B.
\end{aligned}$$

Definition A.0.4 (*j-invariant* of a General Weierstrass Equation)**.** Let R be a (commutative unital) ring. For the general Weierstrass equation (Definition A.0.2)
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$
with coefficients $a_1, a_2, a_3, a_4, a_6 \in R$, the following are standard notation:

The *j-invariant* associated to the Weierstrass equation (assuming Δ is invertible in R) is the element $j \in R$ given by

$$j = \frac{c_4^3}{\Delta},$$

(Notation A.0.3)

For a short Weierstrass equation (Definition A.0.2)

$$y^2 = x^3 + Ax + B,$$

with $A, B \in R$ the j-invariant becomes

$$j = 1728\frac{4A^3}{4A^3 + 27B^2} = 1728\frac{4A^3}{-\frac{\Delta}{16}} = -1728\frac{4A^3}{\Delta/16}.$$

Definition A.0.5. Let R be a Dedekind domain with field of fractions K. Given an elliptic curve E/K, a *Weierstrass model of E over R* is a closed subscheme $W \subseteq \mathbb{P}^2_R$ defined by a (projective) Weierstrass equation (Definition A.0.2) such that W is flat over R, whose generic fiber $W_K = W \times_{\operatorname{Spec} R} \operatorname{Spec} K$ is isomorphic to E as a curve over K.

Definition A.0.6. Let R be a Dedekind domain with field of fractions K and let E/K be an elliptic curve (Definition A.0.1). A *minimal Weierstrass model of E over R* is a Weierstrass model (Definition A.0.5) W of E over R such that for every nonzero prime ideal $\mathfrak{p} \subset R$, the $R_\mathfrak{p}$-model $W_{R_\mathfrak{p}} = W \times_{\operatorname{Spec} R} \operatorname{Spec} R_\mathfrak{p}$ is a Weierstrass model whose discriminant $\Delta(W_{R_\mathfrak{p}})$ has minimal possible $v_\mathfrak{p}$-adic valuation among all Weierstrass models of E over $R_\mathfrak{p}$.

A (either non-homogeneous/affine or homogeneous/projective) Weierstrass equation (Definition A.0.2) yielding a minimal Weierstrass model of E over R would be called a *minimal Weierstrass equation of E/R*.

(♠ TODO: define the ring of S-integers) In the case that R is the ring of integers of a local field, or more generally a DVR, we might call a minimal Weierstrass model a *local minimal Weierstrass model* and the equation a *local minimal Weierstrass equation*. In the case that R has infinitely many prime ideals (e.g. R is the ring of integers or some ring of S-integers of a global field), or more generally more than one nonzero prime ideal, we might call a minimal Weierstrass model a *global minimal Weierstrass model* and the equation a *global minimal Weierstrass equation*.

Appendix B. Conjectures in algebraic geometry

Conjecture B.0.1 (Tate's conjecture, [Tat65, Conjecture 1])**.** Let k be a field that is finitely generated over its prime field. Let k_s be a separable closure of k and let $\operatorname{Gal}(k_s/k)$ be the absolute Galois group of k. Let X/k be a smooth projective variety. Fix a prime number ℓ which is invertible in k. The space

$$H^{2i}(X_{k_s}, \mathbb{Q}_\ell(2i))^{\operatorname{Gal}(k_s/k)}$$

(♠ TODO: define ℓ-adic cohomology of ℓ-adic sheaves) of invariants of the action of $\operatorname{Gal}(k_s/k)$ on the $2i$th ℓ-adic cohomology group $H^{2i}(X_{k_s}, \mathbb{Q}_\ell(2i))$ of the $2i$th Tate twist $\mathbb{Q}_\ell(2i)$ is

spanned, as a $\mathbb{Q}_\ell$-vector space, by the classes of codimension i subvarieties of X. More precisely, the map

$$A^i(X) \otimes \mathbb{Q}_\ell \to H^{2i}(X_{k_s}, \mathbb{Q}_\ell(2i))^{\mathrm{Gal}(k_s/k)}$$

induced by the cycle map(♠ TODO: define cycle map)

$$c^i : Z(X_{k_s}) \to H^{2i}(X_{k_s}, \mathbb{Q}_\ell(2i))$$

is a surjection.

Appendix C. Miscellaneous definitions

Definition C.0.1. A *global field* is a field K that is either:

- a finite extension of the field of rational numbers $\mathbb{Q}$ (i.e., a number field), or
- a finite extension of the field of rational functions $\mathbb{F}_q(t)$ in one variable over a finite field $\mathbb{F}_q$ (i.e., a global function field).

Definition C.0.2 (Abelian variety over a field)**.** Let k be a field. An *abelian variety over k* is a complete, connected algebraic group variety defined over k, i.e.

- A is a smooth, proper, geometrically connected algebraic variety over k,
- A is endowed with a group structure defined by morphisms of varieties over k (multiplication $m : A \times_k A \to A$ and inverse $i : A \to A$),
- the group law satisfies the group axioms scheme-theoretically.

In particular, an abelian variety is a projective algebraic group variety over k.

Appendix D. Selmer groups

Definition D.0.1 (Selmer group for an isogeny of abelian varieties over a global field)**.** (♠ TODO: It should be possible to define this for more general group schemes) Let K be a global field (Definition C.0.1), and let A and B be abelian varieties (Definition C.0.2) defined over K. Suppose $\varphi : A \to B$ is an isogeny defined over K.

Denote by $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K, and by $\mathrm{Sel}^\varphi(A/K)$ (or $\mathrm{Sel}^{(\varphi)}(A/K)$) the *Selmer group of φ over K*, defined as the subgroup of the Galois cohomology group $H^1(K, \ker\varphi)$ given by

$$\mathrm{Sel}^\varphi(A/K) := \ker\left(H^1(K, \ker\varphi) \to \prod_v H^1(K_v, A(\overline{K}))[\varphi] \right),$$

(♠ TODO: define the kummer map associated to φ) where the product runs over all places v of K, and $H^1(K_v, A)[\varphi]$ denotes the image of the local Kummer map associated to φ.

We describe the map

$$H^1(K, \ker\varphi) \to \prod_v H^1(K_v, A(\overline{K}))[\varphi] \tag{A}$$

(♠ TODO: define a decomposition group) used to define the kernel above: for each place v of K, fix an extension v to $\overline{K}$, which yields an embedding $\overline{K} \subset \overline{K}_v$ and a decomposition group $G_v \subset G_K$. Note that G_v acts on $A(\overline{K}_v)$ and $B(\overline{K}_v)$, and the base change φ_v of φ to K_v induces a Kummer short exact sequence

$$0 \to B(K_v)/\varphi(A(K_v)) \xrightarrow{\delta_{\varphi_v}} H^1(G_v, A[\varphi]) \to H^1(G_v, A(\overline{K}_v))[\varphi] \to 0.$$

The natural inclusions $G_v \subset G_K$ and $E(K) \subset E(K_v)$ give restriction maps on cohomology, and we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B'(K)/\varphi(A(K)) & \xrightarrow{\delta_\varphi} & H^1(G_K, A[\varphi]) & \longrightarrow & H^1(G_K, A(\overline{K}))[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v B'(K_v)/\varphi(A(K_v)) & \xrightarrow{\delta_{\varphi_v}} & \prod_v H^1(G_v, A[\varphi]) & \longrightarrow & \prod_v H^1(G_v, A(\overline{K}_v))[\phi] & \longrightarrow & 0 \end{array}$$

The map (A) is the one given in the above commutative diagram.

Appendix E. Heights

Definition E.0.1 (naive height of an elliptic curve over a number field, cf. [Sil89]). (♠ TODO: can this definition be aplicable for a global function field) Let K be a number field. For $a, b \in K$ with $4a^3 + 27b^2 \neq 0$, let $E(a, b)$ be the elliptic curve given by (affine) Weierstrass equation (Definition A.0.2)

$$E(a, b) : y^2 = x^3 + ax + b$$

1. Define the *(naive multiplicative) height of an elliptic curve* E/K to be
$$H(E) = \inf_{\substack{a,b \in K \\ E \cong_K E(a,b)}} H([a^3, b^2, 1])$$
where H is the height function of points in $\mathbb{P}^2(K)$.
2. Define the *(naive logarithmic) height of an elliptic curve* E/K to be
$$h(E) = \inf_{\substack{a,b \in K \\ E \cong_K E(a,b)}} h([a^3, b^2, 1])$$
where h is the logarithmic height function of points in $\mathbb{P}^2(K)$.

References

[Arm92] Brumer Armand. The average rank of elliptic curves i. *Inventiones mathematicae*, 109(1):445–472, 1992.

[BH12] Salman Baig and Chris Hall. Experimental data for goldfeld's conjecture over function fields. *Experimental Mathematics*, 21(4):362–374, 2012.

[BLGHT11] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi–Yau varieties and potential automorphy ii. *Publications of the Research Institute for Mathematical Sciences*, 47(1):29–98, 2011.

[BS15a] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Annals of Mathematics*, pages 191–242, 2015.

[BS15b] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of Mathematics*, pages 587–621, 2015.

[BSD65] Bryan John Birch and Peter Francis Swinnerton-Dyer. Notes on elliptic curves. ii. *Journal für die reine und angewandte Mathematik*, 218:79–108, 1965.

[CHT08] Laurent Clozel, Michael Harris, and Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l galois representations. *Publications mathématiques*, 108:1–181, 2008.

[FLR23] Tony Feng, Aaron Landesman, and Eric M. Rains. The geometric distribution of Selmer groups of elliptic curves over function fields. *Mathematische Annalen*, 387:615–687, 2023.

[Gol06] Dorian Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number Theory Carbondale 1979: Proceedings of the Southern Illinois Number Theory Conference Carbondale, March 30 and 31, 1979*, pages 108–118. Springer, 2006.

[HB04] David Heath-Brown. The average analytic rank of elliptic curves. *Duke Math. J.*, 122:591–623, 2004.

[HSBT05] Michael Harris, Nick Shepherd-Barron, and Richard Taylor. Ihara's lemma and potential automorphy, 2005.

[Jor05] Andrei Jorza. The birch and swinnerton-dyer conjecture for abelian varieties over number fields, 2005.

[KM23] Seoyoung Kim and M. Ram Murty. From the Birch and Swinnerton-Dyer conjecture to Nagao's conjecture. *Mathematics of Computation*, 92(339):385–408, 2023.

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45. American Mathematical Society, 1999.

[Nag97] Koh-ichi Nagao. Q(t)-rank of elliptic curves and certain limit coming from the local points. *Manuscripta mathematica*, 92(1):13–32, 1997.

[Poo18] Bjorn Poonen. Heuristics for the arithmetic of elliptic curves. In *Proceedings of the International Congress of Mathematicians: Rio de Janeiro 2018*, pages 399–414. World Scientific, 2018.

[PR12] BJORN POONEN and ERIC RAINS. Random maximal isotropic subspaces and selmer groups. *Journal of the American Mathematical Society*, 25(1):245–269, 2012.

[RS98] Michael Rosen and Joseph H. Silverman. On the rank of an elliptic surface. *Inventiones mathematicae*, 133:43–67, 1998.

[Sil89] Joseph H. Silverman. Elliptic curves of bounded degree and height. *Proceedings of the American Mathematical Society*, 105(3):540–545, 1989.

[Tat65] John T. Tate. Algebraic cycles and poles of zeta functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 93–110. Harper & Row, 1965. Also in Collected works of John Tate (2 vols.), Amer. Math. Soc. (2016), vol. 2.

[Tat66] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki : années 1964/65 1965/66, exposés 277-312*, number 9 in Astérisque, pages 415–440. Société mathématique de France, 1966. talk:306.

[Tay08] Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l galois representations. ii. *Publications mathématiques*, 108:183–239, 2008.

[You06] Matthew Young. Low-lying zeros of families of elliptic curves. *Journal of the American Mathematical Society*, 19(1):205–250, 2006.