Talk 12: The Mordell-Weil theorem

One of the highlight of early 20th century's arithmetic geometry is the proof of the Mordell[1]-Weil[2] theorem. The statement is quite simple:

Theorem 0.1 Let K be a number field, i.e. a finite extension of $\mathbb{Q}$. Let E/K be an elliptic curve. Then the group $E(K)$ is finitely generated.

Corollary 0.2 $E(K) \cong \mathbb{Z}^r \times E_{\text{tors}}(K)$, where $E_{\text{tors}}(K)$ is the torsion part of the group. The number r is uniquely determined and is called the **rank** of E.

1 Weak Mordell-Weil theorem

We firstly consider a key ingredient of the proof of Mordell-Weil theorem.

Theorem 1.1 (Weak Mordell-Weil) Let K be a number field, E/K an elliptic curve defined over K. Then for any $m \geq 2$ an integer, the group $E(K)/mE(K)$ is finite.

We will do two reductions to prove the theorem. Firstly we could assume $E[m] \subset E(K)$ completely. Then we mimic the Kummer theory for Galois fields and consider

$$L := K\left([m]^{-1}E(K)\right) \tag{1.1}$$

ranging over all m-th roots of $E(K)$ in $E\left(\bar{K}\right)$ and reduce to show L/K is finite.

We introduce an important proposition in Galois cohomology. This simplifies the proof a lot.

Lemma 1.2 (Inflation-Restriction sequence) Let M be a $G_{\bar{K}/K}$-module and L/K a finite Galois extension. Then M is a $G_{\bar{K}/L}$-module and we have

$$\text{res} : H^1\left(G_{\bar{K}/K}, M\right) \to H^1\left(G_{\bar{K}/L}, M\right) \tag{1.2}$$

Further as $G_{\bar{K}/L}$ normal in $G_{\bar{K}/K}$, the submodule of invariants $M^{G_{\bar{K}/L}}$ has a $G_{L/K}$-module structure. By precomposing the quotient map $G_{\bar{K}/K} \to G_{L/K}$ we get

$$\text{inf} : H^1\left(G_{L/K}, M^{G_{\bar{K}/L}}\right) \to H^1\left(G_{\bar{K}/K}, M\right) \tag{1.3}$$

The sequence

$$0 \to H^1\left(G_{L/K}, M^{G_{\bar{K}/L}}\right) \xrightarrow{\text{inf}} H^1\left(G_{\bar{K}/K}, M\right) \xrightarrow{\text{res}} H^1\left(G_{\bar{K}/L}, M\right) \tag{1.4}$$

is exact.

[1] Louis Mordell(1888-1972)
[2] André Weil(1906-1998)

Lemma 1.3 Let L/K be a finite Galois extension, suppose $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is finite.

Proof: The inclusion $E(K) \hookrightarrow E(L)$ induces a natural map

$$E(K)/mE(K) \xrightarrow{\varphi} E(L)/mE(L) \tag{1.5}$$

Define $A = \ker \varphi = \frac{E(K) \cap mE(K)}{mE(K)}$, The exact sequence of $G_{\bar{K}/K}$-modules

$$0 \to E[m] \to E(\bar{K}) \xrightarrow{[m]} E(\bar{K}) \to 0 \tag{1.6}$$

induces a long exact sequence

$$\begin{aligned} 0 \to H^0\left(G_{\bar{K}/K}, E[m]\right) \to H^0\left(G_{\bar{K}/K}, E(\bar{K})\right) \xrightarrow{[m]} H^0\left(G_{\bar{K}/K}, E(\bar{K})\right) \\ \xrightarrow{\delta} H^1\left(G_{\bar{K}/K}, E[m]\right) \to H^1\left(G_{\bar{K}/K}, E(\bar{K})\right) \xrightarrow{[m]} H^1\left(G_{\bar{K}/K}, E(\bar{K})\right) \to \dots \end{aligned} \tag{1.7}$$

This turns out to be

$$0 \to E(K)[m] \to E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} \dots \tag{1.8}$$

Splitting in the middle gives us a short exact sequence

$$0 \to E(K)/mE(K) \xrightarrow{\delta} H^1\left(G_{\bar{K}/K}, E[m]\right) \to H^1\left(G_{\bar{K}/K}, E(\bar{K})\right)[m] \to 0 \tag{1.9}$$

Apply this general theory and Lemma 1.2 we have the following commutative diagram(assuming $E[m] \subset E(L)$):

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & E(K)/mE(K) & \longrightarrow & E(L)/mE(L) \\ & & \big\downarrow & & \big\downarrow \delta & & \big\downarrow \delta \\ 0 & \longrightarrow & H^1\left(G_{L/K}, E[m]\right) & \xrightarrow{\text{inf}} & H^1\left(G_{\bar{K}/K}, E[m]\right) & \xrightarrow{\text{res}} & H^1\left(G_{\bar{L}/L}, E[m]\right) \end{array}$$

The finiteness of $H^1\left(G_{L/K}, E[m]\right)$ implies the lemma immediately. ■

Definition 1.4 (Kummer[3] pairing)Let $m \geq 2$ an integer,

$$\begin{aligned} \kappa : E(K) \times G_{\bar{K}/K} &\to E[m] \\ (P, \sigma) &\mapsto \kappa(P, \sigma) = Q^\sigma - Q \end{aligned} \tag{1.10}$$

where $Q \in E(\bar{K})$ such that $[m]Q = P$.

Proposition 1.5 Let κ be the Kummer pairing defined above.
1. κ is well-defined, independent of the choice of Q.

[3]Ernst Eduard Kummer(1810-1893)

2. κ is bilinear, the kernel of κ on the left is $mE(K)$ and on the right is $G_{\bar{K}/L}$, where $L := K([m]^{-1}E(K))$ adjoining all $Q \in E(\bar{K})$ such that $[m]Q \in E(K)$.

Hence $\kappa : E(K)/mE(K) \times G_{L/K} \to E[m]$ is a perfect pairing.

Proof: Suppose $E[m] \subset E(K)$, then the $G_{\bar{K}/K}$-action on it is trivial and

$$H^1\left(G_{\bar{K}/K}, E[m]\right) \cong \mathrm{Hom}_{\mathrm{Grp}}\left(G_{\bar{K}/K}, E[m]\right) \tag{1.11}$$

By general homological algebra, the connecting homomorphism in the proof of Lemma 1.3 is given by: for each $P \in E(K)$ find $Q \in E(\bar{K})$ such that $[m]Q = P$, then define the 1-cocycle representing $\delta(P)$ as

$$\begin{aligned} c : G_{\bar{K}/K} &\to E[m], \\ c(\sigma) &= Q^\sigma - Q \end{aligned} \tag{1.12}$$

Since δ is well-define, so is κ. Now since $E(K)/mE(K) \xrightarrow{\delta} H^1\left(G_{\bar{K}/K}, E[m]\right)$ is an injection, it suffices to show the kernel of κ on the right is $G_{\bar{K}/L}$.

Suppose $\sigma \in G_{\bar{K}/L}$, then as $Q \in E(L)$ we have $\kappa(P, \sigma) = Q^\sigma - Q = O$. Conversely if $\kappa(P, \sigma) = O, \forall P$, then σ fixes all points $Q \in E(\bar{K})$ with $[m]Q \in E(K)$ and by definition, the field L.

Finally notice that $G_{\bar{K}/L}$ is normal and L/K is therefore a Galois extension. ■

Remark 1.6 In fact, upon computing the rank and torsion points of $E(K)$, deciding which morphism in $\mathrm{Hom}\left(G_{L/K}, E[m]\right)$ comes from $E(K)/mE(K)$ is the only inefficient part of the algorithm. Since $G_{L/K}$ can be determined completely and the generator of $E(K)$ is deduced from height function assuming the set $E(K)/mE(K)$ is known.

Suppose Birch and Swinnerton-Dyer conjecture is ture, then Manin[4] [1] proposed an efficient algorithm to determine this.

Recall from the last talk, a **good reduction** of E/K for K a local field has a minimal Weierstrass equation with $v(\Delta) = 0$. In case of K a global field, we say E/K has a good reduction at v a finite place of K, if E/K_v has a good reduction.

Remark 1.7 In general E/K doesn't possess a Weierstrass equation that is minimal at every finite place v. It's however possible for $K = \mathbb{Q}$(in fact for all number fields with class number 1).

Another good news is that for any Weierstrass equation of E/K, all but finitely many places have the property $v(a_i) \geq 0$ and $v(\Delta) = 0$.

We reuse the following lemma from last talk.

[4] Yuri Manin(1937-2023)

Lemma 1.8 Let v be a discrete valuation on K s.t. $v(m) = 0$. Let K_v be the completion and k_v the residue field, then the reduction map

$$E(K)[m] \longrightarrow \tilde{E}(k_v) \tag{1.13}$$

is injective.

As the torsion group $E[m]$ is finite and Kummer pairing is perfect, we just need to show L/K is a finite extension and this completes the proof of Theorem 1.1.

Proposition 1.9
1. L/K is an abelian extension with exponent m.
2. Define

$$\begin{aligned} S = \{v \in M_K^\infty\} \cup \big\{v \in M_k^0 : E \text{ has a bad reduction at } v\big\} \\ \cup \big\{v \in M_K^0 : v(m) \neq 0\big\} \end{aligned} \tag{1.14}$$

then S is finite and L/K is unramified outside of S.

Proof: 1 is clear from the injection $G_{L/K} \hookrightarrow \mathrm{Hom}(E(K), E[m])$.

Let's pick a $Q \in E(\bar{K})$ with $[m]Q \in E(K)$, we show $K' := K(Q)$ is unramified at $v \notin s$. Now let $v' \in M_{K'}^0$ a place lying above v and $k'_{v'}/k_v$ the residue field extension. As E has good reduction at v, it also has a good reduction at v', hence the reduction map $E(K') \to \tilde{E}(k'_{v'})$ is well-defined.

Consider the inertia group(by Chebotarev density theorem well defined) $I_{v'/v} \subset G_{\bar{K}/K}$ of v'/v, by definition $\sigma \in I_{v'/v}$ acts trivially on $\tilde{E}(k'_{v'})$, thus for $Q \in E(K')$,

$$\widetilde{Q^\sigma - Q} = \tilde{Q}^\sigma - \tilde{Q} = O \tag{1.15}$$

and

$$[m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = O \tag{1.16}$$

hence by Lemma 1.8 $Q^\sigma - Q = O$, and $K(Q)$ is unramified at v'. Since v' is arbitrary, this completes the proof. ■

Now we apply the general theorem of Kummer extension.

Proposition 1.10 Let K be a number field, $S \subset M_K$ a finite set of places containing M_K^∞. Let $m \geq 2$ and L/K the maximal abelian extension with exponent m. If L/K is unramified outside of S, then L/K is finite.

2 Height functions and descent

The weak Mordell-Weil theorem solely is not enough to imply $E(K)$ is finitely generated. A simple but convincing example is $\mathbb{R}/m\mathbb{R}$, which is finite($= 0$) for any integer, but $\mathbb{R}$ is definitely not a finitely generated $\mathbb{Z}$-module. We can divide arbitrary large power of m in $\mathbb{R}$, we want to show this is not the case for $E(K)$.

The idea is to attach a height for every point in $E(K)$ and show that multiplication increases height in a "controlled" way, with finitely many "bounded" points.

Remark 2.1 This is not new in mathematics. Fermat[5] already used the method of infinite descent to solve number theory problems, including the famous Fermat's last theorem in case $n = 4$.

Theorem 2.2 (General descent) Let A be an abelian group, $h : A \to \mathbb{R}$ a height function with following properties:

1. For every $Q \in A$, there is a constant $C_1(Q)$ such that
$$h(P+Q) \leq 2h(P) + C_1(Q), \forall P \in A \tag{2.1}$$
2. There's an integer $m \geq 2$ and C_2 depending only on A such that
$$h([m]P) \leq m^2 h(P) - C_2, \forall P \in A \tag{2.2}$$
3. For any constant C_3 the set
$$\{P \in A : h(P) \leq C_3\} \tag{2.3}$$
is finite.

Suppose further that for m in 2, the group A/mA is finite, then A is finitely generated.

Sketch of proof: Choose $Q_1, ..., Q_r \in A$ representing A/mA. For any $P \in A$ we show the difference of P and a $\mathbb{Z}$-linear combination of Q_i is a multiple of a point whose height is smaller that a constant independent $C := 1 + \frac{1}{2}(C_1' + C_2)$ of P, where $C_1' = \max\{C_1(-Q_i)\}$. This implies that $Q_1, ..., Q_r$ together with $\{P \in A : h(P) \leq C\}$ generates the group A.

Write $t \in \mathbb{Q}$ as $t = \frac{p}{q}$ in the simplest form and we define $H(t) := \max\{|p|, |q|\}$.

Definition 2.3 Let $E/\mathbb{Q}$ with Weierstrass equation $E : y^2 = x^3 + Ax + B, A, B \in \mathbb{Z}$. The **logarithmic height** of $E(\mathbb{Q})$ is
$$\begin{gathered} h_x : E(\mathbb{Q}) \to \mathbb{R}, \\ h_x(P) = \begin{cases} \log H(x(P)) & \text{if } P \neq O \\ 0 & \text{if } P = O \end{cases} \end{gathered} \tag{2.4}$$

We verify this is the height function with $m = 2$.

Lemma 2.4 Let $E/\mathbb{Q}$ be an elliptic curve,

[5] Pierre de Fermat(1607-1665)

1. for any $Q \in E(\mathbb{Q})$ there exists a constant $C_1(Q)$ with
$$h_x(P+Q) \leq 2h_x(P) + C_1(Q), \forall P \in E(\mathbb{Q}) \tag{2.5}$$
2. there's a constant C_2 such that
$$h_x([2]P) \leq 4h_x(P) - C_2, \forall P \in E(\mathbb{Q}) \tag{2.6}$$
3. for any C_3 constant the set
$$\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\} \tag{2.7}$$
is finite.

Theorem 2.5 (Mordell) Let $E/\mathbb{Q}$ be an elliptic curve, then the rational points $E(\mathbb{Q})$ are finitely generated.

We will now define a general height function on projective spaces, this also gives us more insight on the properties of elliptic curves later.

A naîve approach on $\mathbb{P}^N(\mathbb{Q})$ would be: as $\mathbb{Z}$ a PID in $\mathbb{Q}$, we can find a homogenous coordinate $P = [x_0, ..., x_N]$ with $x_i \in \mathbb{Z}$ coprime, then the height is just the maximum of absolute values of all coordinates.

This does not work for general number fields as the ring of integers is not always a PID(that's why we need class field theory). Instead for $P \in \mathbb{P}^N(K), P = [x_0, ..., x_N], x_i \in K$ we define
$$H_K(P) := \prod_{v \in M_K} \max\{|x_0|_v, ..., |x_N|_v\}^{n_v} \tag{2.8}$$
where $n_v := [K_v : \mathbb{Q}_v]$ the local degree of K at v.

Proposition 2.6 This height $H_K(P)$ is independent of the choice of coordinates, $H_K(P) \geq 1$ and for L/K a finite extension, $H_L(P) = H_K(P)^{[L:K]}$.

Inspired by the last proposition we can define a height on the whole $\mathbb{P}^N(\bar{\mathbb{Q}})$.

Definition 2.7 Let $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$, the **absolute height** of P, denoted by $H(P)$, is, by choosing a number field K such that $P \in \mathbb{P}^N(K)$, $H(P) = H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}$.

Note from the definition it's quite easy to see there're only finite points with bounded height on projective spaces. We collect some properties of this height function.

Proposition 2.8
1. Let $F : \mathbb{P}^N(\bar{\mathbb{Q}}) \to \mathbb{P}^M(\bar{\mathbb{Q}})$ be a morphism of degree d, then there exists constants C_1, C_2 such that

$$C_1 H(P)^d \leq H(F(P)) \leq C_2 H(P)^d \tag{2.9}$$

2. Let $f(T) = a_0 T^d + a_1 T^{d-1} + ... + a_d = a_0 (T - \alpha_1) ... (T - \alpha_d) \in \bar{\mathbb{Q}}[T]$, then

$$2^{-d} \prod_{j=1}^{d} H([\alpha_j, 1]) \leq H([a_0, ..., a_d]) \leq 2^{d-1} \prod_{j=1}^{d} H([\alpha_j, 1]) \tag{2.10}$$

3. $H(P)$ is invariant under the Galois action, i.e. for $\sigma \in G_{\bar{\mathbb{Q}}/\mathbb{Q}}$, we have

$$H(P^\sigma) = H(P), \forall P \in \mathbb{P}^N(\bar{\mathbb{Q}}) \tag{2.11}$$

4. Let C, d be constants, the set

$$\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) : H(P) \leq C, [\mathbb{Q}(P) : \mathbb{Q}] \leq d\} \tag{2.12}$$

   is finite. In particular,

$$\{P \in \mathbb{P}^N(K) : H_K(P) \leq C\} \tag{2.13}$$

   is finite for K a number field.

On elliptic curves, we want to turn this multiplicative relation into an additive one. Recall that if $f \in \bar{K}(E)$ is a non-constant function, then f defines a surjective morphism

$$\begin{aligned} f : E(\bar{K}) &\to \mathbb{P}^1(\bar{K}), \\ P &\mapsto \begin{cases} [1, 0] & \text{if } P \text{ is a pole of } f \\ [f(P), 1] & \text{otherwise} \end{cases} \end{aligned} \tag{2.14}$$

Definition 2.9 Let E/K be a elliptic curve, the **height** on E relative to $f \in \bar{K}(E)$ is the function

$$\begin{aligned} h_f &: E(\bar{K}) \to \mathbb{R} \\ h_f(P) &= \log H(f(P)) \end{aligned} \tag{2.15}$$

If we choose $f \in K(x)$, i.e. f is even, then we can show for any $P, Q \in E$,

$$h_f(P + Q) + h_f(P - Q) = 2h_f(P) + 2h_f(Q) + \mathcal{O}(1) \tag{2.16}$$

From this equality we can easily deduce the desired descent property of h_f.

Theorem 2.10 (Mordell-Weil) Let E/K be an elliptic curve for K a number field, then $E(K)$ is finitely generated.

The equation (2.16) reminds us of quadratic forms. A natural question is: can we find a canonical height function that is also a quadratic form? The answer is surely yes.

Definition 2.11 (Néron[6]-Tate[7] height) Let $f \in K(x)$ be an even function, the **canonical height** $\hat{h}$ on E/K is

$$\hat{h} : E(\bar{K}) \to \mathbb{R}$$
$$\hat{h}(P) = \frac{1}{\deg(f)} \lim_{N \to \infty} 4^{-N} h_f([2^N]P) \tag{2.17}$$

Proposition 2.12
1. $\hat{h}$ is well-defined, the limit converges and is independent of the choice of f.
2. $\hat{h}$ is a quadratic form on $E(\bar{K})$.
3. Let $P \in E(\bar{K})$, then $\hat{h}(P) \geq 0$ and $\hat{h}(P) = 0$ iff P is a torsion point.
4. Let $g \in K(x)$ an even function, then

$$(\deg g)\hat{h} = h_g + \mathcal{O}(1) \tag{2.18}$$

Moreover, $\hat{h}$ is the unique quadratic form on $E(\bar{K})$ satisfying 4.

3 Outlook

The Mordell-Weil theorem didn't end one research field, however it opened a whole zoo with active research.

By Corollary 0.2 we want to determine the rank and torsion part for any elliptic curve E/K. The torsion part is easy to handle.

Theorem 3.1 (Mazur[8]) Let $E/\mathbb{Q}$ be an elliptic curve, then $E_{\text{tors}}(\mathbb{Q})$ is isomorphic to one of the following:

$$\begin{gathered} \mathbb{Z}/N\mathbb{Z}, 1 \leq N \leq 10, N = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2M\mathbb{Z}, 1 \leq M \leq 4 \end{gathered} \tag{3.1}$$

Theorem 3.2 (Merel[9]) For every $d \geq 1$ an integer there's $N(d)$ constant such that for all $[K : \mathbb{Q}] \leq d$ and E/K any elliptic curve, one has

$$|E_{\text{tors}}(\mathbb{K})| \leq N(d) \tag{3.2}$$

It's however, not so easy to determine the rank of $E(K)$.

Conjecture 3.3 There exists $E/\mathbb{Q}$ of arbitrary large rank.

[6] André Néron(1922-1985)
[7] John Tate(1925-2019)
[8] Barry Mazur(1937-)
[9] Loïc Merel(1965-)

A strong evidence leads people to believe this conjecture is the proof of the analogous theorem in the case of function fields by Shafarevich[10] and Tate [3].

Perhaps one of the most prominent conjectures about the rank of elliptic curves is the Birch[11] and Swinnerton-Dyer[12] conjecture.

Let E/K be an elliptic curve on a number field K. Let $v \in M_K$ be a finite place where E has a good reduction. Recall we have proven the Weil conjecture for elliptic curves, this turns the zeta function $Z(\tilde{E}/k_v; T)$ into a rational function

$$Z(\tilde{E}/k_v; T) = \frac{L_v(T)}{(1-T)(1-q_v T)} \tag{3.3}$$

where $L_v(T) = 1 - a_v T + q_v T^2$ and $q_v = \#k_v, a_v = q_v + 1 - \#\tilde{E}(k_v)$.

We extend this also into finite places with bad reductions such that in any case we have

$$L(v)(1/q_v) = \#\tilde{E}_{\text{ns}}(k_v)/q_v \tag{3.4}$$

with $\tilde{E}_{\text{ns}}(k_v)$ is the non-singular part of the reduction.

Definition 3.4 The ***L*-series** of E/K is defined by the Euler product

$$L_{E/K}(s) = \prod_{v \in M_K^0} L_v(q_v^{-s})^{-1} \tag{3.5}$$

This series converges and defines an analytic function for $\mathrm{Re}(s) > \frac{3}{2}$.

It is conjectured that the L-series contains rich information about the global arithmetic properties of E/K.

Conjecture 3.5 (Birch and Swinnerton-Dyer) Let $E/\mathbb{Q}$ be an elliptic curve, then $L_E(s)$ has a zero at $s = 1$ of order equal to the rank of $E(\mathbb{Q})$.

Bibliography

[1] J. I. Manin, “Cyclotomic Fields and Modular Curves,” *Russ. Math. Surv.*, vol. 26, no. 6, pp. 7–78, Dec. 1971, doi: 10.1070/RM1971v026n06ABEH001272.

[2] J. H. Silverman, *The Arithmetic of Elliptic Curves*, vol. 106. in Graduate Texts in Mathematics, vol. 106. New York, NY: Springer New York, 2009. doi: 10.1007/978-0-387-09494-6.

[3] J. Tate and I. R. Shafarevich, “The rank of elliptic curves,” in *Doklady Akademii Nauk USSR*, 1967, pp. 770–773.

[10] Igor Shafarevich(1923-2017)
[11] Bryan John Birch(1931-)
[12] Peter Swinnerton-Dyer(1927-2018)