Complete 2-descent を用いた楕円曲線のモーデル・ヴェイユ群の計算について

池田愛輝

自然科学研究科数理物質科学専攻
博士前期課程 2 年

2020 年 2 月 7 日

修士論文について

修士論文の内容

- 第 1 章: 第 2 章以降の準備
  (楕円曲線の諸性質, ガロアコホモロジー, 降下定理, クンマー理論)
- 第 2 章: モーデル・ヴェイユ群のねじれ部分群の計算
  (形式群, 還元写像)
- 第 3 章: モーデルの定理
  (弱モーデル・ヴェイユの定理, 高さ関数)
- 第 4 章: モーデル・ヴェイユ群 $E(\mathbb{Q})$ の計算
  (m-Descent, Complete 2-descent, 例 4.3)

Complete 2-descent とよばれる定理が主題

発表の流れ

§1 イントロダクション

§2 Complete 2-descent

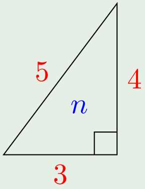
§3 モーデル・ヴェイユ群 $E(\mathbb{Q})$ の計算例

合同数問題

定義 (合同数)

$\mathbb{N} \ni n$ が合同数であるとは, ある直角三角形の面積となるときをいう.

合同数の例 (6 は合同数)



$$3^2 + 4^2 = 5^2,$$
$$n = 3 \cdot 4 \cdot \frac{1}{2} = 6.$$

各辺が 3, 4, 5 の直角三角形が存在するので, 6 は合同数.

合同数問題: $\mathbb{N} \ni n$ はいつ合同数か？

合同数の例 (5, 7 は合同数)

(1) 5 は合同数である (フィボナッチ, 1170–1240).

$$\because \left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \frac{1681}{36} = \left(\frac{41}{6}\right)^2, \quad \frac{3}{2}\cdot\frac{20}{3}\cdot\frac{1}{2} = 5.$$

(2) 7 は合同数である (オイラー, 1707–1783).

$$\because \left(\frac{35}{12}\right)^2 + \left(\frac{24}{5}\right)^2 = \frac{113569}{3600} = \left(\frac{337}{60}\right)^2, \quad \frac{35}{12}\cdot\frac{24}{5}\cdot\frac{1}{2} = 7.$$

合同数の例 (5, 7 は合同数)

(1) 5 は合同数である (フィボナッチ, 1170–1240).

$$\because \left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \frac{1681}{36} = \left(\frac{41}{6}\right)^2, \quad \frac{3}{2}\cdot\frac{20}{3}\cdot\frac{1}{2} = 5.$$

(2) 7 は合同数である (オイラー, 1707–1783).

$$\because \left(\frac{35}{12}\right)^2 + \left(\frac{24}{5}\right)^2 = \frac{113569}{3600} = \left(\frac{337}{60}\right)^2, \quad \frac{35}{12}\cdot\frac{24}{5}\cdot\frac{1}{2} = 7.$$

定理 (合同数問題の言い換え)

$n \in \mathbb{N}$ に対し, 次は同値:

(a) n は合同数;

(b) 楕円曲線 $y^2 = x^3 - n^2 x$ に無限個の解 $x, y \in \mathbb{Q}$ が存在.

代数体 K 上の楕円曲線

定義 (代数体 K 上の楕円曲線, 判別式 Δ)

$a_2, a_4, a_6 \in K$ に対して

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

で定義された曲線を K 上の楕円曲線 E という. ただし,

$$\Delta := -64a_2^3a_6 + 16a_2a_4^2 - 64a_4^3 - 432a_6^2 + 288a_2a_4a_6 \neq 0$$

をみたす.

有理数体 $\mathbb{Q}$ 上の楕円曲線の例

- $E : y^2 = x^3 - n^2x \ (n \in \mathbb{N})$
- $E : y^2 = x(x-12)(x-36)$

興味の対象

定義 (楕円曲線 E 上の K 有理点 P)

P の座標がすべて K の元であるとき, K 有理点とよぶ.

K 有理点の例 ($K = \mathbb{Q}$)

$E : y^2 = x(x-12)(x-36)$ に対し,
$(0,0)$, $(12,0)$, $(36,0)$ は $\mathbb{Q}$ 有理点.

問題 (興味の対象: K 有理点)

楕円曲線 $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ の K 有理点をすべて求めよ.

動機:

- 有理点の有無を知りたい代数多様体
(cf. 合同数問題への応用)
- K 有理点を求める一般的な方法は知られていない

興味の対象

定義 (楕円曲線 E 上の K 有理点 P)

P の座標がすべて K の元であるとき, K 有理点とよぶ.

K 有理点の例 ($K = \mathbb{Q}$)

$E : y^2 = x(x-12)(x-36)$ に対し,
$(0,0)$, $(12,0)$, $(36,0)$ は $\mathbb{Q}$ 有理点.

問題 (興味の対象: K 有理点)

楕円曲線 $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ の K 有理点をすべて求めよ.

動機:

- 有理点の有無を知りたい代数多様体
  (cf. 合同数問題への応用)
- K 有理点を求める一般的な方法は知られていない

興味の対象

定義 (楕円曲線 E 上の K 有理点 P)

P の座標がすべて K の元であるとき, K 有理点とよぶ.

K 有理点の例 ($K=\mathbb{Q}$)

$E: y^2 = x(x-12)(x-36)$ に対し,
$(0,0)$, $(12,0)$, $(36,0)$ は $\mathbb{Q}$ 有理点.

問題 (興味の対象: K 有理点)

楕円曲線 $E: y^2 = x^3 + a_2x^2 + a_4x + a_6$ の K 有理点をすべて求めよ.

動機:

- 有理点の有無を知りたい代数多様体
  (cf. 合同数問題への応用)
- K 有理点を求める一般的な方法は知られていない

モーデル・ヴェイユ群 $E(K)$

定義 (モーデル・ヴェイユ群 $E(K)$)

楕円曲線 E の K 有理点全体からなる集合に無限遠点 O を付け加えた集合

$$E(K) := \{(x, y) \in E \mid x, y \in K\} \cup \{O\}$$

を E の**モーデル・ヴェイユ群**という.

定理 (楕円曲線 E の群構造)

(1) $E \cup \{O\}$ は O を単位元とするアーベル群.
(2) $E(K)$ は $E \cup \{O\}$ の部分群.

$m \in \mathbb{N}$ と楕円曲線 E に対して, 次のように記号を定める:

$$E[m] := \{P \in E \mid [m]P = O\},$$
$$E(K)_{\mathrm{tors}} : E(K) \text{ のねじれ (位数有限) 部分群.}$$

定理 (モーデルの定理, 1922)

$E(\mathbb{Q})$ は有限生成アーベル群である. i.e.,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$$

となる $r \geq 0$ が一意に存在する.

定義 (モーデル・ヴェイユ群 $E(\mathbb{Q})$ の階数 rank(E))

$$\mathrm{rank}(E) := r$$

- ねじれ部分群 $E(\mathbb{Q})_{\mathrm{tors}}$ を求めることは比較的簡単
- 一般に rank(E) を求めることは難しい

定理 (モーデルの定理, 1922)

$E(\mathbb{Q})$ は有限生成アーベル群である. i.e.,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$$

となる $r \geq 0$ が一意に存在する.

定義 (モーデル・ヴェイユ群 $E(\mathbb{Q})$ の階数 rank(E))

$$\text{rank}(E) := r$$

- ねじれ部分群 $E(\mathbb{Q})_{\text{tors}}$ を求めることは比較的簡単
- 一般に rank(E) を求めることは難しい
- $E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^t \times (\mathbb{Z}/l\mathbb{Z})^{s_l} \times \mathbb{Z}^{\text{rank}(E)} \ (t \geq 0)$

  $\Rightarrow \#(E(\mathbb{Q})/2E(\mathbb{Q})) = 2^{t+\text{rank}(E)}$

定理 (モーデルの定理, 1922)

$E(\mathbb{Q})$ は有限生成アーベル群である. i.e.,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$$

となる $r \geq 0$ が一意に存在する.

定義 (モーデル・ヴェイユ群 $E(\mathbb{Q})$ の階数 rank(E))

$$\mathrm{rank}(E) := r$$

- ねじれ部分群 $E(\mathbb{Q})_{\mathrm{tors}}$ を求めることは比較的簡単
- 一般に rank(E) を求めることは難しい
- $E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^t \times (\mathbb{Z}/l\mathbb{Z})^{s_l} \times \mathbb{Z}^{\mathrm{rank}(E)}$ $(t \geq 0)$

  $\Rightarrow \#(E(\mathbb{Q})/2E(\mathbb{Q})) = 2^{t+\mathrm{rank}(E)}$

rank(E) の計算 $\longleftrightarrow \#(E(\mathbb{Q})/2E(\mathbb{Q}))$ と $E(\mathbb{Q})_{\mathrm{tors}}$ の計算

$\rightsquigarrow$ 以下, $\underline{\#E(\mathbb{Q})/2E(\mathbb{Q}) \text{ を求めることを目標とする}}$

m-Descent への準備

重要な点：

- 楕円曲線 E と $m \in \mathbb{N}$ から "悪い素点" からなる有限集合 $S_{E,m}$ が定まる
- $S_{E,m}$ から "分かりやすい" 有限群 $K(S_{E,m})$ が定まる

定義

楕円曲線 E と $m \in \mathbb{N}$ に対して,

$$S_{E,m} := \{\mathfrak{p} \in M_K^0 \mid \mathrm{ord}_{\mathfrak{p}}(m) > 0 \text{ または } \mathrm{ord}_{\mathfrak{p}}(\Delta_E) > 0\},$$

$$K(S_{E,m}) := \{b \mod (K^*)^m \in K^*/(K^*)^m \mid b \in K^*, \quad \mathrm{ord}_{\mathfrak{p}}(b) \equiv 0 \bmod m \ (\forall \mathfrak{p} \in M_K^0 \setminus S_{E,m})\}.$$

- K: 代数体, K^*: K の乗法群, I_K: K のイデアル群
- M_K^0: K の有限素点全体, $\mathrm{ord}_{\mathfrak{p}} : I_K \longrightarrow \mathbb{Z} \cup \{\infty\}$: $M_K^0 \ni \mathfrak{p}$ の正規離散付値

定理 (m-Descent)

E を $E[m] \subset E(K)$ である K 上の楕円曲線とする.

(1) 左非退化な双線形写像

$$B : E(K)/mE(K) \times E[m] \longrightarrow K(S_{E,m})$$

が存在する.

(2) $T \in E[m]$ に対し, $f_T \in K(E)$ が

(i) $f_T \circ [m] = g_T^m \ (\exists g_T \in E(K))$,

(ii) $\mathrm{div}(f_T) = m(T) - m(O)$

をみたすなら, 次が成り立つ:

$$B(P,T) = f_T(P) \bmod (K^*)^m$$
$$(\forall T \in E[m], \forall P \in E(K) \setminus \{T, O\}) \,.$$

注意: m-Descent $\rightsquigarrow$ Complete 2-descent (後述)

定理 (m-Descent)

E を $E[m] \subset E(K)$ である K 上の楕円曲線とする.

(1) 左非退化な双線形写像

$$B : E(K)/mE(K) \times E[m] \longrightarrow K(S_{E,m})$$

が存在する.

(2) $T \in E[m]$ に対し, $f_T \in K(E)$ が

(i) $f_T \circ [m] = g_T^m \ (\exists g_T \in E(K))$,
(ii) $\mathrm{div}(f_T) = m(T) - m(O)$

をみたすなら, 次が成り立つ:

$$B(P,T) = f_T(P) \bmod (K^*)^m$$
$$(\forall T \in E[m], \forall P \in E(K) \setminus \{T,O\}).$$

注意: m-Descent $\rightsquigarrow$ Complete 2-descent (後述)

定理 (m-Descent)

E を $E[m] \subset E(K)$ である K 上の楕円曲線とする.

(1) 左非退化な双線形写像

$$B : E(K)/mE(K) \times E[m] \longrightarrow K(S_{E,m})$$

が存在する.

(2) $T \in E[m]$ に対し, $f_T \in K(E)$ が

(i) $f_T \circ [m] = g_T^m \ (\exists g_T \in E(K))$,
(ii) $\operatorname{div}(f_T) = m(T) - m(O)$

をみたすなら, 次が成り立つ:

$$B(P,T) = f_T(P) \bmod (K^*)^m$$
$$(\forall T \in E[m], \forall P \in E(K) \setminus \{T, O\}) .$$

注意: m-Descent $\rightsquigarrow$ Complete 2-descent (後述)

m-Descent を $m=2$ で適用

楕円曲線 $E: y^2=(x-e_1)(x-e_2)(x-e_3)$ $(e_i\in K)$ に対し，
$T_1:=(e_1,0)$, $T_2:=(e_2,0)$ とおくと $E[2]=\langle T_1,T_2\rangle$.

- m-Descent における左非退化な双線形写像 B より，

$$
\begin{aligned}
L_B: E(K)/2E(K) &\hookrightarrow \mathrm{Hom}(E[2],K(S_{E,2}));\\
P &\longmapsto B(P,*)
\end{aligned}
$$

- $E[2]=\langle T_1,T_2\rangle$ より，

$$
\begin{aligned}
\Psi:\mathrm{Hom}(E[2],K(S_{E,2})) &\xrightarrow{\cong} K(S_{E,2})\times K(S_{E,2});\\
\rho &\longmapsto (\rho(T_1),\rho(T_2))
\end{aligned}
$$

- T_i $(i=1,2)$ に対して，$f_{T_i}:=(x-e_i)\in K(E)$ は
  - $f_{T_i}\circ[2]=g_{T_i}^2$ $(\exists g_{T_i}\in K(E))$,
  - $\mathrm{div}(f_{T_i})=2(T_i)-2(O)$

  をみたす (m-Descent (2) における条件を f_{T_i} はみたす)

$\to \Phi:=\Psi\circ L_B$ と定義し，計算．

定理 (Complete 2-descent)

$e_1, e_2, e_3 \in K$ により定義された楕円曲線

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

に対し, 単射準同型

$$\exists \Phi : E(K)/2E(K) \hookrightarrow K(S_{E,2}) \times K(S_{E,2})$$

s.t., $\forall (b_1, b_2) \in K(S_{E,2}) \times K(S_{E,2}) \setminus \{\Phi(O), \Phi(T_1), \Phi(T_2)\}$ に対し, 次は同値となる:

(a) $(b_1, b_2) \in \mathrm{Im}(\Phi)$;

(b) 変数 z_1, z_2, z_3 に関する方程式

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1 \end{cases}$$

に解 $(z_1, z_2, z_3) \in K^* \times K^* \times K$ が存在.

重要な点: (1) $\#E(K)/2E(K) = \#\mathrm{Im}(\Phi)$;
(2) (b): $\mathrm{Im}(\Phi)$ に入る判定条件.

定理 (Complete 2-descent)

$e_1, e_2, e_3 \in K$ により定義された楕円曲線

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

に対し, 単射準同型

$$\exists \Phi : E(K)/2E(K) \hookrightarrow K(S_{E,2}) \times K(S_{E,2})$$

s.t., $\forall (b_1, b_2) \in K(S_{E,2}) \times K(S_{E,2}) \setminus \{\Phi(O), \Phi(T_1), \Phi(T_2)\}$ に対し, 次は同値となる:

(a) $(b_1, b_2) \in \mathrm{Im}(\Phi)$;

(b) 変数 z_1, z_2, z_3 に関する方程式

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1 \end{cases}$$

に解 $(z_1, z_2, z_3) \in K^* \times K^* \times K$ が存在.

重要な点: (1) $\#E(K)/2E(K) = \#\mathrm{Im}(\Phi)$;
(2) (b): $\mathrm{Im}(\Phi)$ に入る判定条件.

定理 (Complete 2-descent)

$e_1, e_2, e_3 \in K$ により定義された楕円曲線

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

に対し, 単射準同型

$$\exists \Phi : E(K)/2E(K) \hookrightarrow K(S_{E,2}) \times K(S_{E,2})$$

s.t., $\forall (b_1, b_2) \in K(S_{E,2}) \times K(S_{E,2}) \setminus \{\Phi(O), \Phi(T_1), \Phi(T_2)\}$ に対し, 次は同値となる:

(a) $(b_1, b_2) \in \mathrm{Im}(\Phi)$;

(b) 変数 z_1, z_2, z_3 に関する方程式

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1 \end{cases}$$

に解 $(z_1, z_2, z_3) \in K^* \times K^* \times K$ が存在.

重要な点: (1) $\#E(K)/2E(K) = \#\mathrm{Im}(\Phi)$;
(2) (b): $\mathrm{Im}(\Phi)$ に入る判定条件.

§3 モーデル・ヴェイユ群 $E(\mathbb{Q})$ の計算例

Complete 2-descent の適用

$$E : y^2 = x(x-12)(x-36)$$

に対し, $\mathbb{Q}(S_{E,2}) = T := \{\pm 1, \pm 2, \pm 3, \pm 6\} \leq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

$$\exists \Phi : E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow T \times T$$

s.t., $\forall (b_1, b_2) \in T \times T \setminus \{\Phi(O), \Phi((0,0)), \Phi((12,0))\}$
に対し, 次は同値である:

(a) $(b_1, b_2) \in \mathrm{Im}(\Phi)$;

(b) 変数 z_1, z_2, z_3 に関する方程式

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = 12 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = 36 \end{cases}$$

に解 $(z_1, z_2, z_3) \in K^* \times K^* \times K$ が存在.

以下, $(b_1, b_2) \in T \times T$ をとり (b) を考察! $\rightsquigarrow \#\mathrm{Im}(\Phi)$

- Step 1: $b_1 < 0$ かつ $b_2 > 0$ のとき

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = 12 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = 36 \end{cases}$$

に解が存在しない．実際，もし存在したとすれば

$$0 > b_1 z_1^2 = b_2 z_2^2 + 12 > 0$$

で矛盾．$\times$: $(b_1, b_2) \notin \mathrm{Im}(\Phi)$ を表す $\longrightarrow$

▶ Step 1: $b_1 < 0$ かつ $b_2 > 0$ のとき

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = 12 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = 36 \end{cases}$$

に解が存在しない．実際，もし存在したとすれば

$$0 > b_1 z_1^2 = b_2 z_2^2 + 12 > 0$$

で矛盾．×: $(b_1, b_2) \notin \mathrm{Im}(\Phi)$ を表す $\longrightarrow$

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1					×	×	×	×
2					×	×	×	×
3					×	×	×	×
6					×	×	×	×
-1								
-2								
-3								
-6								

▶ Step 2: $(b_1, b_2) = (1, -2)$ のとき

$$\begin{cases} z_1^2 + 2z_2^2 = 12 \\ z_1^2 + 2z_3^2 = 36 \end{cases}$$

を $(z_1, z_2, z_3) = (2, 2, 4)$ はみたす.
$\therefore$ Complete 2-descent $\rightsquigarrow$ $(1, -2) \in \mathrm{Im}(\Phi)$.
○: $(b_1, b_2) \in \mathrm{Im}(\Phi)$ を表す $\longrightarrow$

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1					×	×	×	×
2					×	×	×	×
3					×	×	×	×
6					×	×	×	×
-1								
-2								
-3								
-6								

▶ Step 2: $(b_1, b_2) = (1, -2)$ のとき

$$\begin{cases} z_1^2 + 2z_2^2 = 12 \\ z_1^2 + 2z_3^2 = 36 \end{cases}$$

を $(z_1, z_2, z_3) = (2, 2, 4)$ はみたす.

$\therefore$ Complete 2-descent $\rightsquigarrow$ $(1, -2) \in \mathrm{Im}(\Phi)$.

○: $(b_1, b_2) \in \mathrm{Im}(\Phi)$ を表す $\longrightarrow$

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1					×	×	×	×
2					×	×	×	×
3					×	×	×	×
6					×	×	×	×
-1								
-2	○							
-3								
-6								

- **Step 3: 新たな × を得る**

Step 1 より $(-1,1),(-1,2),(-1,3),(-1,6) \notin \mathrm{Im}(\Phi)$,
Step 2 より $(1,-2) \in \mathrm{Im}(\Phi)$.

$$
\begin{aligned}
(1,-2)\cdot(-1,1) &= (-1,-2) \quad \mathrm{Im}(\Phi),\\
(1,-2)\cdot(-1,2) &= (-1,-1) \quad \mathrm{Im}(\Phi),\\
(1,-2)\cdot(-1,3) &= (-1,-6) \quad \mathrm{Im}(\Phi),\\
(1,-2)\cdot(-1,6) &= (-1,-3) \quad \mathrm{Im}(\Phi).
\end{aligned}
$$

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1					×	×	×	×
2					×	×	×	×
3					×	×	×	×
6					×	×	×	×
-1								
-2	○							
-3								
-6								

- **Step 3: 新たな × を得る**

  Step 1 より $(-1,1),(-1,2),(-1,3),(-1,6) \notin \mathrm{Im}(\Phi)$,
  Step 2 より $(1,-2) \in \mathrm{Im}(\Phi)$.

$$
\begin{aligned}
(1,-2)\cdot(-1,1) &= (-1,-2) \notin \mathrm{Im}(\Phi),\\
(1,-2)\cdot(-1,2) &= (-1,-1) \notin \mathrm{Im}(\Phi),\\
(1,-2)\cdot(-1,3) &= (-1,-6) \notin \mathrm{Im}(\Phi),\\
(1,-2)\cdot(-1,6) &= (-1,-3) \notin \mathrm{Im}(\Phi).
\end{aligned}
$$

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1					×	×	×	×
2					×	×	×	×
3					×	×	×	×
6					×	×	×	×
-1								
-2	○							
-3								
-6								

Step 3: 新たな $\times$ を得る

Step 1 より $(-1,1), (-1,2), (-1,3), (-1,6) \notin \mathrm{Im}(\Phi)$,
Step 2 より $(1,-2) \in \mathrm{Im}(\Phi)$.

$$
\begin{aligned}
(1,-2)\cdot(-1,1) &= (-1,-2) \notin \mathrm{Im}(\Phi),\\
(1,-2)\cdot(-1,2) &= (-1,-1) \notin \mathrm{Im}(\Phi),\\
(1,-2)\cdot(-1,3) &= (-1,-6) \notin \mathrm{Im}(\Phi),\\
(1,-2)\cdot(-1,6) &= (-1,-3) \notin \mathrm{Im}(\Phi).
\end{aligned}
$$

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1					×	×	×	×
2					×	×	×	×
3					×	×	×	×
6					×	×	×	×
-1					×			
-2	○				×			
-3					×			
-6					×			

このような議論を Step 1 – Step 13 まで行い, 次を得る:

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1	○	×	○	×	×	×	×	×
2	×	×	×	×	×	×	×	×
3	×	×	×	×	×	×	×	×
6	○	×	○	×	×	×	×	×
-1	×	×	×	×	×	×	×	×
-2	○	×	○	×	×	×	×	×
-3	○	×	○	×	×	×	×	×
-6	×	×	×	×	×	×	×	×

- $\#(E(\mathbb{Q})/2E(\mathbb{Q})) = \#\mathrm{Im}(\Phi) = 8 = 2^3$
- ねじれ部分群の議論より $E(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$

$\longrightarrow 2^{\mathrm{rank}(E)+2} = \#(E(\mathbb{Q})/2E(\mathbb{Q})) = 2^3$

$\longrightarrow \mathrm{rank}(E) + 2 = 3$

$\longrightarrow \mathrm{rank}(E) = 1$

このような議論を Step 1 – Step 13 まで行い, 次を得る:

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1	○	×	○	×	×	×	×	×
2	×	×	×	×	×	×	×	×
3	×	×	×	×	×	×	×	×
6	○	×	○	×	×	×	×	×
-1	×	×	×	×	×	×	×	×
-2	○	×	○	×	×	×	×	×
-3	○	×	○	×	×	×	×	×
-6	×	×	×	×	×	×	×	×

- $\#(E(\mathbb{Q})/2E(\mathbb{Q})) = \#\mathrm{Im}(\Phi) = 8 = 2^3$
- ねじれ部分群の議論より $E(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$
  $\longrightarrow 2^{\mathrm{rank}(E)+2} = \#(E(\mathbb{Q})/2E(\mathbb{Q})) = 2^3$
  $\longrightarrow \mathrm{rank}(E) + 2 = 3$
  $\longrightarrow \mathrm{rank}(E) = 1$

このような議論を Step 1 – Step 13 まで行い, 次を得る:

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1	○	×	○	×	×	×	×	×
2	×	×	×	×	×	×	×	×
3	×	×	×	×	×	×	×	×
6	○	×	○	×	×	×	×	×
-1	×	×	×	×	×	×	×	×
-2	○	×	○	×	×	×	×	×
-3	○	×	○	×	×	×	×	×
-6	×	×	×	×	×	×	×	×

- $\#(E(\mathbb{Q})/2E(\mathbb{Q})) = \#\mathrm{Im}(\Phi) = 8 = 2^3$
- ねじれ部分群の議論より $E(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$

$\longrightarrow 2^{\mathrm{rank}(E)+2} = \#(E(\mathbb{Q})/2E(\mathbb{Q})) = 2^3$

$\longrightarrow \mathrm{rank}(E) + 2 = 3$

$\longrightarrow \mathrm{rank}(E) = 1$

このような議論を Step 1 – Step 13 まで行い, 次を得る:

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1	○	×	○	×	×	×	×	×
2	×	×	×	×	×	×	×	×
3	×	×	×	×	×	×	×	×
6	○	×	○	×	×	×	×	×
-1	×	×	×	×	×	×	×	×
-2	○	×	○	×	×	×	×	×
-3	○	×	○	×	×	×	×	×
-6	×	×	×	×	×	×	×	×

- $\#(E(\mathbb{Q})/2E(\mathbb{Q})) = \#\mathrm{Im}(\Phi) = 8 = 2^3$
- ねじれ部分群の議論より $E(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$

$\longrightarrow 2^{\mathrm{rank}(E)+2} = \#(E(\mathbb{Q})/2E(\mathbb{Q})) = 2^3$

$\longrightarrow \mathrm{rank}(E) + 2 = 3$

$\longrightarrow \mathrm{rank}(E) = 1$

このような議論を Step 1 – Step 13 まで行い，次を得る:

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1	○	×	○	×	×	×	×	×
2	×	×	×	×	×	×	×	×
3	×	×	×	×	×	×	×	×
6	○	×	○	×	×	×	×	×
-1	×	×	×	×	×	×	×	×
-2	○	×	○	×	×	×	×	×
-3	○	×	○	×	×	×	×	×
-6	×	×	×	×	×	×	×	×

- $\#(E(\mathbb{Q})/2E(\mathbb{Q})) = \#\mathrm{Im}(\Phi) = 8 = 2^3$
- ねじれ部分群の議論より $E(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$

  $\longrightarrow 2^{\mathrm{rank}(E)+2} = \#(E(\mathbb{Q})/2E(\mathbb{Q})) = 2^3$

  $\longrightarrow \mathrm{rank}(E) + 2 = 3$

  $\longrightarrow \mathrm{rank}(E) = 1$

このような議論を Step 1 – Step 13 まで行い, 次を得る:

$b_2 \backslash b_1$	1	2	3	6	-1	-2	-3	-6
1	◯	×	◯	×	×	×	×	×
2	×	×	×	×	×	×	×	×
3	×	×	×	×	×	×	×	×
6	◯	×	◯	×	×	×	×	×
-1	×	×	×	×	×	×	×	×
-2	◯	×	◯	×	×	×	×	×
-3	◯	×	◯	×	×	×	×	×
-6	×	×	×	×	×	×	×	×

- $\#(E(\mathbb{Q})/2E(\mathbb{Q})) = \#\mathrm{Im}(\Phi) = 8 = 2^3$
- ねじれ部分群の議論より $E(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$

  $\longrightarrow 2^{\mathrm{rank}(E)+2} = \#(E(\mathbb{Q})/2E(\mathbb{Q})) = 2^3$

  $\longrightarrow \mathrm{rank}(E) + 2 = 3$

  $\longrightarrow \mathrm{rank}(E) = 1$

$E(\mathbb{Q})$ の計算例 (例 4.5)

$\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x(x-12)(x-36)$ に対し

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$$

である.

$E(\mathbb{Q})$ の計算例 (例 4.5)

$\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x(x-12)(x-36)$ に対し

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$$

である.

今後の課題

- $\#E(\mathbb{Q})[2] = 4$ のとき $\#E(\mathbb{Q})/2E(\mathbb{Q})$ の計算
- $E : y^2 = x^3 - p^2 x$ は $\mathrm{rank}(E) \geq 1$ か？
- BSD 予想と保型形式