アーベル多様体の有理等分点について

小川 裕之 (大阪大学大学院 理学研究科)

§1 序文

(a) いきなりですが, 定理をひとつ.

定理 1.1 (Mordell-Weil) k を有限次代数体とし, A を k 上定義されたアーベル多様体とする. このとき, A の k-有理点の全体 $A(k)$ (Mordell-Weil 群) は有限生成アーベル群である.

アーベル多様体について学び始めてすぐに習う定理のひとつと思います. 多様体の有理点は適当な連立方程式系の解で, 有限個の生成元を求めればすべての解がわかるわけです. 例えとして適切ではないかもしれませんが, Pell 方程式の解の全体が二次体の単数群に関係し, 基本解 (基本単数) から簡単な手続きですべての解が得られることに似ています. Mordell-Weil 群の生成元を具体的に求めることができるでしょうか. "アーベル多様体とその点の記述方法" を考え, "有理点をすべて見つけるアルゴリズム" を作る. 有理数体上の楕円曲線 (1 次元アーベル多様体) の場合でもまだ完全ではありません. 問いを少し易しくして, "自由部分の階数がどの程度であるか" とか, "ねじれ部分群としてどの様な群が現れるか" とか, "等分点の位数としてどの様な数が現れるか" とか. 自由部分の階数については, "幾らでも階数の大きな, 有理数体上定義された楕円曲線が存在するだろう" と思われていますが, "有理数体上定義された楕円曲線の階数は上に有界であろう" と相反する予想もあります. どちらもそれなりに言い分があります. 階数にはあまり深入りせず, Mordell-Weil 群のねじれ部分群について話します.

(b) アーベル多様体の等分点は, 類体の構成など重要な対象ですが, 図形的にも面白い. 有理数体上定義された楕円曲線の場合, 例外点 (exceptional point) というものがありました. 楕円曲線上のある点 P_0 から始めて, その点での接線が元の楕円曲線と交わる点 P_1 とおく. P_1 での接線が再び楕円曲線と交わる点を P_2 とおきます. 以下これを繰り返して, 楕円曲線上の点を取り続けます. 点の列が周期的になるとき P_0 を例外点と言いました. 例外点でなければ, 楕円曲線上の有理点がどんどん見つかります. 周期の長い例外点を探す過程で, 加法群としての楕円曲線が詳しく調べられました. 各回の操作は楕円曲線の -2 倍写像で, 例外点は等分点に当たります. 例外点の周期の長さの探求は, "有理数体上定義されたすべての楕円曲線について, 等分の位数は有界か?" (Kubert) という上限予想につながりました. 結局,

定理 1.2 (Mazur) (Springer LNM 601 (1977), 107–148) 楕円曲線 $E/\mathbb{Q}$ に対して, $\mathbb{Q}$-有理等分点全体 $E(\mathbb{Q})_{\mathrm{tors}}$ は次の群のいずれかに同型である : $\mathbb{Z}/n\mathbb{Z}$ $(n = 1, 2, 3, \cdots, 9, 10, 12)$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ $(m = 1, 2, 3, 4)$

これら 15 個の群が実際に現れることは具体的に計算すればできますが, これら以外の群が現れないことを証明するのは非常に大変なことです. Billing-Mahler (J. London Math. Soc. 15 (1940), 32–43), Ogg (Invent. Math. 12 (1971), 105–111), Mazur-Tate (Invent. Math. 22 (1973/74), 41–49) らによって, 与えられた自然数が有理等分点の位数として現れないことを証明する方法が確立されました. Ogg (Bull. Amer. Math. Soc. 81, 1975) が上の 15 個に限ると予想し, Mazur が証明しました.

(c) 次に向かうべき方向は, 定義体をより大きな次数の代数体に取ることと, 次元の高いアーベル多様体を扱うことの 2 つ考えられます. 定義体の次数を上げる方向でも, 次の様に予想されました.

予想 1.3 (楕円曲線の上限予想) 自然数 d にのみ依存する定数 $B(d)$ が存在し, 次が成り立つ : d 次代数体 k 上定義された楕円曲線 E に対して, E の k-有理等分点の位数は $B(d)$ を越えない.

Kenku-Momose (Nagoya Math. J. 109 (1988), 125–149) によって, 二次体上定義された楕円曲線の有理等分点群の取り得る形 (25 個) が得られ, 更に 17 以上の素数位数等分点が存在しないなら, その 25 個に限ることが示されました. また, 幾つかの素数について, その位数の等分点が存在しないことも示されました. Kamienny (Bull. Amer. Math. Soc. 23 (1990), no. 2, 371–373 / Invent. Math. 109 (1992), no. 2, 221–229) により, "二次体上定義された楕円曲線において, 有理等分点の位数の素因子は 13 以下である" ことが示され,

定理 1.4 (Kamienny-Kenku-Momose)　2 次体 k 上定義された楕円曲線の有理等分点のなす群は, 次のいずれかに同型である：　$\mathbb{Z}/n\mathbb{Z}$　$(n = 1, 2, \cdots, 14, 16, 18)$,　$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$　$(m = 1, 2, \cdots, 6)$,
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z}$　$(m = 1, 2 \quad k = \mathbb{Q}(\sqrt{-3}))$,　$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$　$(k = \mathbb{Q}(\sqrt{-1}))$

Kamienny は, 二次体のときの流れを踏まえて, "楕円曲線の有理等分点の素因子は, 定義体の次数にのみ依存する定数を上限にもつだろう" と, 上限予想より少し弱い予想を考えました. Kamienny-Mazur (Astérisque No. 228 (1995), 3, 81–100) は, Kamienny の予想から上限予想が従うことを示し, $d \leq 8$ について Kamienny の予想が成り立つことを示しました. Abramovich (Astérisque No. 228 (1995), 3, 5–17) は, Kamienny-Mazur の方法を精密化して $d \leq 12$ について上限予想が正しいことを示しました. 結局, Merel (Invent. Math. 124 (1996), no. 1–3, 437–449) により, d 次代数体について, 楕円曲線の有理等分点の位数の素因子は $(1 + 3^{d/2})^2$ 以下であることが示されました.

定理 1.5 (Merel)　すべての自然数 d に対して, 上限 $B(d)$ が存在する. つまり, 楕円曲線の上限予想は正しい.

Parent (J. Reine Angew. Math. 506 (1999), 85–116) は, Merel 結果から $B(d)$ の効率的な上界を与るために, 素数ベキ位数の等分点に関する評価を与えました. 煩雑になりますが, Merel の結果と合わせると, $B(d)$ の具体的な評価式が得られます.

定理 1.6 (Parent)　d 次代数体上定義された楕円曲線について, 有理等分点の位数が p^n ($p \geq 5$ は素数) であるなら, $p^n \leq 65\,(3^d - 1)\,(2d)^6$ が成り立つ.

(d)　アーベル多様体の次元を上げる方向には, 余り多くの結果は得られていません. ともかく想定されるのは, 次の一般上限予想でしょう.

予想 1.7 (一般上限予想)　自然数 d, g にのみ依存する定数 $B(d, g)$ が存在し, 次が成り立つ：　d 次代数体 k 上定義された絶対既約な g 次元アーベル多様体 A に対して, A の k-有理等分点の位数は $B(d, g)$ を越えない.

虚数乗法をもつアーベル多様体に限るなら, Silverberg (Contemp. Math. 133 (1992), 175–193) により,

定理 1.8 (Silverberg)　アーベル多様体として虚数乗法をもつもののみを考えるとき, 上限予想は正しい. 特に, 虚数乗法をもつ有理数体上定義された 2 次元アーベル多様体について, 有理等分点の位数は 185640 を越えない.

一般的には殆ど何も得られておらず, 良し悪しは別にして, 楕円曲線で例外点と言って楽しんでいたころの様なのんびりした雰囲気にあるようです. 以下, §2 で代数曲線の因子類群について話します. Torelli の定理により, 3 次元以下の (絶対既約な) アーベル多様体は非特異完備代数曲線のヤコビ多様体に同型であるので, 代数曲線の因子類群に限定してもそれほど不都合はないでしょう. 一般のアーベル多様体で加法を扱うのはとても大変なのですが, 因子類群の加法なら Riemann-Roch の定理を使って, 楕円曲線と同じ感覚で計算できるでしょう. §3 で位数の高い有理等分点探索の記録について話し, それらのもとになった Leprévost による位数の高い有理因子類を見つける方法を §4 で解説します.

§2　有理因子類

(a)　k を有限次代数体とし, $\overline{k}$ をその代数閉包とする. ガロア群を $G_k = \mathrm{Gal}(\overline{k}/k)$ とおく. C を k 上定義された非特異完備代数曲線とし, その種数を $g = g(C)$ とする. C の点で生成された自由アーベル群を C の因子類群 $\mathrm{Div}(C)$ という. 任意の因子 $D \in \mathrm{Div}(C)$ は, C の各点ごとにまとめた和 $D = \sum e_P P$　$(e_P \in \mathbb{Z})$ に表すことができる. すべての係数 e_P が非負の因子 D を整因子といい, $D \geq 0$ と書く. 因子 D の係数の和 $\deg D = \sum e_P$ を D の次数といい, 次数が 0 の因子の全体を $\mathrm{Div}^0(C)$ と書く. $\overline{k}(C)$ を C の函数体とする. 有理函数 $\varphi \in \overline{k}(C)^\times$ の因子を $\mathrm{div}(\varphi)$ と書く. 函数の因子を主因子といい, 主因子全体のなす群 $\mathrm{Div}^\ell(C)$ を主因子群という. 主因子の次数は 0 なので, 主因子群は $\mathrm{Div}^0(C)$ の部分群である. $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Div}^\ell(C)$ を因子類群 (Picard 群) という. 因子 D の属する因子類を $[D]$ と書く.

(b)　代数曲線 C として k 上定義された物を取ったので, ガロア群 G_k の作用を考えることができる. これまで単に C の点というときには, 座標が $\overline{k}$ に含まれるものを考えていた. 点の各座標に G_k を作用させることで, C の点の全体に G_k が働く. この作用で不変な点 $P \in C$ を k-有理点と呼び, k-有理点の全体を $C(k)$ と書く. C への

G_k の作用が因子群に自然に延びる. G_k-不変な因子を k-有理因子といい, k-有理因子の全体を $\mathrm{Div}(C)(k)$ と書く. $\mathrm{Div}(C)(k) \subset \mathrm{Div}(C)$ は G_k-不変な部分群である. 因子の次数はガロア群の作用で変わらないので, $\mathrm{Div}^0(C) \subset \mathrm{Div}(C)$ も G_k-不変な部分群である. 有理函数の係数への作用により, G_k は函数体にも働く. G_k-不変な有理函数を k 上定義された有理函数といい. k 上定義された有理函数の全体を $k(C)$ と書く. 任意の $\sigma \in G_k$ に対して $\mathrm{div}(\varphi)^\sigma = \mathrm{div}(\varphi^\sigma)$ が成り立つので, 主因子群 $\mathrm{Div}^\ell(C) \subset \mathrm{Div}(C)$ も G_k-不変な部分群である. $\mathrm{Div}^0(C)$ も $\mathrm{Div}^\ell(C)$ も G_k-不変だったので, 因子類群 $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Div}^\ell(C)$ に自然にガロア群 G_k が作用する. 実際 $\sigma \in G_k$, $[D] \in \mathrm{Pic}^0(C)$ に対して, $[D]^\sigma = [D^\sigma]$ で σ の作用が定まる. G_k-不変な因子類を k-有理因子類といい, k-有理因子類の全体を $\mathrm{Pic}^0_k(C)$ とおき, k-有理因子類群という.

(c) Riemann-Roch の定理より, 種数 $g = g(C)$ が 0 のとき 0 次の因子は主因子になり ($\mathrm{Div}^0(C) = \mathrm{Div}^\ell(C)$), 因子類群 $\mathrm{Pic}^0(C)$ は消える. 以下, 種数は 1 以上とする. 因子類群 $\mathrm{Pic}^0(C)$ は C のヤコビ多様体 $J(C)$ (の $\overline{k}$-有理点全体のなす群) に同型で, $\mathrm{Pic}^0_k(C)$ はその k-有理点群 $J(C)(k)$ である. ヤコビ多様体は $g = g(C)$ 次元の k 上定義されたアーベル多様体なので, Mordell-Weil の定理により k-有理因子類群 $\mathrm{Pic}^0_k(C)$ は有限生成アーベル群になる. 位数が有限の因子類を等分点 (あるいは, ねじれ因子類) といい, 位数が有限の k-有理因子を k-有理等分点という. $\mathrm{Pic}^0_k(C)$ のねじれ部分群を $\mathrm{Pic}^0_k(C)_{\mathrm{tors}}$ と書き, k-有理等分点群という.

(d) 点 $P_0 \in C$ を任意にとる. C から $\mathrm{Pic}^0(C)$ への写像 $\Phi_{P_0} : C \ni P \longmapsto [P - P_0] \in \mathrm{Pic}^0(C)$ を (P_0 を基点とする) 基準写像という.

Riemann-Roch の定理より, 種数が 1 なら Φ_{P_0} は単射になる. Φ_{P_0} により C は $\mathrm{Pic}^0(C)$ に (部分多様体として) 埋め込まれる. 曲線 C の n 個の対称積を $\mathrm{Sym}^n(C)$ とおく. $\mathrm{Sym}^n(C)$ は n 次の整因子の全体に等しい. n 次の因子 D_0 に対して, 写像 $\Phi_{D_0} : \mathrm{Sym}^n(C) \ni D \longmapsto [D - D_0] \in \mathrm{Pic}^0(C)$ が定義できる. Φ_{D_0} を D_0 を基点とする (一般) 基準写像という. Riemann-Roch の定理より, $n \geq g$ のとき Φ_{D_0} は全射になる. 特に $g = 1$ のとき, 基準写像 $\Phi_{P_0} : C \to \mathrm{Pic}^0(C)$ は C からヤコビ多様体 $J(C)$ への代数多様体の同型写像を引き起こす. ヤコビ多様体 (因子類群) の加法演算が, 基準写像を通して, 種数 1 の代数曲線 C の上に定義される. C の加法演算における零元は P_0 なので, 結局のところ, 種数 1 の代数曲線 C に零元 P_0 を指定することでアーベル多様体 (C, P_0) $(= J(C) = \mathrm{Pic}^0(C))$ が定まる. 同じ様に, 種数 g の非特異完備代数曲線 C に対して, g 次の (整) 因子 D_0 を指定することで, 因子類群 $\mathrm{Pic}^0(C)$ の加法演算を $\mathrm{Sym}^g(C)$ の上に描くことができる. ただし, 種数が 2 以上の場合 Φ_{D_0} は単射でないので因子類の代表としての $\mathrm{Sym}^g(C)$ の元の選び方を指定する必要がある. 殆どの点で (余次元 1 以下の部分多様体の和を除いて) 単射なので, 計算機に載せるのでなければ, あまり神経質にならなくてもちょっと手を動かしてみればすぐに見分けがつくようになるでしょう. 最も簡単な場合だが, 種数が 2 のものをまとめておく.

命題 2.1 C を種数が 2 の超楕円曲線とし, 無限遠点 ∞ は超楕円対合に関して不変とする. 2 次の因子として 2∞ をとると, $\Phi_{2\infty}$ は $\Phi_{2\infty}^{-1}(0)$ を除いて 1 対 1 に対応する. 更に $\Phi_{2\infty}^{-1}(0) = \{P + P' \in \mathrm{Sym}^2(C)\} \simeq \mathbb{P}^1$ である.

基準写像を使って, 因子類の代表として次数 g の整因子を取った. 2 点 $P, Q \in C$ に対して, 因子類 $[P - Q]$ をパケットという. 種数が 2 のとき, 因子類の代表としてパケットを取ることができる. 基準写像は基点の選び方に依存する. パケットで代表を取ると, 基点の様なものに依存せず, 因子類の点を表せる. 一般の種数 (偶数の方が易しい) に対しても, パケットの和, あるいは $g/2$ 次の整因子のパケットを考えれば, 基点によらない因子類の記述ができる.

命題 2.2 C を種数が 2 の非特異完備曲線とし, 写像 $\Psi : C \times C \ni (P, Q) \longmapsto [P - Q] \in \mathrm{Pic}^0(C)$ を考える. このとき Ψ は全射で, $\Psi^{-1}(0) = \{(P, P) \in C \times C\} \simeq C$ を除いて 2 対 1 に対応する.

(e) n 次整因子の全体 $\mathrm{Sym}^n(C)$ に自然に G_k が作用する. G_k-不変な n 次整因子の全体を $\mathrm{Sym}^n_k(C)$ とおく. $D_0 \in \mathrm{Sym}^n_k(C)$ をとる. 基準写像 $\Phi_{D_0} : \mathrm{Sym}^n(C) \to \mathrm{Pic}^0(C)$ について, $\mathrm{Sym}^n_k(C)$ の像は k-有理因子類群 $\mathrm{Pic}^0_k(C)$ に含まれる.

§3 位数の高い有理等分点探索の記録

ここでは, 定義体は有理数体 $\mathbb{Q}$ か 1 変数有理函数体 $\mathbb{Q}(t)$ 上定義された非特異完備代数曲線で, 位数の高い有理等分点をもつものの構成についてまとめます. 一般上限予想 (予想 1.7) で言うなら $B(1, g)$ の下界を与えることにな

ります. 上限 $B(1,g)$ が種数 g に関してどの様な変動をするか眺めることができるかもしれない. 1 変数つき ($\mathbb{Q}(t)$ 上) で考えるのは, 等分点のモジュライ空間に射影直線などの多様体が ($\mathbb{Q}$ 上で) 埋め込まれているかどうかなど, モジュライ空間の様子を垣間見たい. あるいは, ともかく $\mathbb{Q}$ 上定義されるものをたくさん作って楽しみたい.

一般上限予想では絶対既約なアーベル多様体に限定していますが, 楕円曲線の直積など絶対既約でないものも許せば $B(d,g) \geq B(d,1)^g + O(1)$ となります. $B(d,g)$ は有理等分点群に含まれる最大位数の上限なので, 互いに素な有理点を選ぶ必要があるので誤差項 $O(1)$ を含んでいます. 誤差項の評価を良くすることもできますが, 余り意味がないので書きません. また, 代数体上の楕円曲線の線形制限 (scalar restriction) を考えれば $B(d,g) \geq B(dg,1)$ などの評価も得られます.

E. V. Flynn (J. Number Theory 36 (1990), no. 3, 257–265) は, $\mathbb{Q}(t)$ 上定義された種数が g の超楕円曲線で位数が $2g^2+g+1$ の有理等分点をもつものを作りました. 特に $g=2$ のとき $2\times 2^2+2+1=11$ なので, 有理数体上定義された楕円曲線の有理等分点として現れない, 位数 11 の有理等分点を得ました.

F. Leprévost (C. R. Acad. Sci. Paris Ser. I Math. 313 (1991), no. 7, 451–454 / no. 11, 771–774) は, 有理等分点を作り出すうまい手続きを与え, それを使って種数が 2 のときに位数 13, 15, 17, 19, 21 の有理等分点をもつ超楕円曲線の 1 パラメータ族を作りました. その手続きを一般種数に拡げ, Leprv́ost (Manuscripta Math. 75 (1992), no. 3, 303–326) は, 種数が g の超楕円曲線で位数が $2g^2+2g+1$ のものと $2g^2+3g+1$ のものの 1 パラメータ族を作りました. 次節 (§4) でその方法を説明します. 更に Leprévost (C. R. Acad. Sci. Paris Sér. I Math. 316 (1993), no. 8, 819–821) は, 一つか二つずつですが, $22 \sim 29$ の等分点をもつ, 種数 2 の $\mathbb{Q}$ 上の超楕円曲線を作りました. これらの幾つかはそのヤコビ多様体が絶対既約ではないのですが, 29 等分点をもつものは絶対既約になっています. ここで得られた下限 $B(1,2) \geq 29$ は, $B(1,2)$ について現在最良のものです.

Ogawa (Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), no. 9, 295–298) は, Leprévost の方法を真似て, 23 等分点をもつ超楕円曲線の 1 パラメータ族を作りました. 単に作るだけでなく問題意識として 2 のことを指摘しました. ひとつはこの節の始めにある絶対既約の必要性で, もうひとつは, パラメータ族が等分点のモジュライ空間で退化していないことを井草不変量を使って確かめることです.

Leprévost (Manuscripta Math. 92 (1997), no. 1, 47–63) は, $\mathbb{Q}$ 上で位数が $2g(2g+1)$ の有理等分点をもつ超楕円曲線と, $2g^2+5g+5$ の有理等分点をもつ超楕円曲線を作りました. $g \geq 3$ では $B(1,g) \geq 2g(2g+1)$ が下限として現在知られている最良のものです.

Leprévost (Forum Math. 12 (2000), no. 3, 315–364) は, 絶対既約でないものについても, 曲線のヤコビ多様体という条件下でなら自明とは言い切れないことから, 絶対既約のものとは区別して有理等分点の位数の評価を問うた. 種数 2 で 63 等分点, 種数 3 で 60 等分点をもつものを作っています. 絶対既約でない場合は有理等分点群が幾つもの巡回群の直積に分かれるので, 有理等分点群の位数としては, 種数 2 のとき位数 128, 種数 3 のとき位数 864 のものが得られています. 2 個の楕円曲線の直積で, 位数が $12\times 7=84$ の有理等分点や $10\times 9=90$ の有理等分点をもつものが作れ, 3 個の楕円曲線の直積では, 位数が $12\times 7\times 5=420$ や $10\times 9\times 7=630$ のものが作れます. 有理等分点群の位数としては g 個の直積で $(2\times 8)^g = 16^g$ のものが作れます. それらが曲線のヤコビ多様体 (に同種) なものとして作れるかどうかはわかっていません. 絶対既約などの条件をつけても, 有理等分点の位数の上限は殆ど同じではないかと思われていますので, これらの数が $B(d,g)$ の値の目標値になるかもしれません.

§4 Leprèvost の方法

(a) Leprévost は, 位数の高い有理等分点をもつ超楕円曲線を見つける方法を考えました. 楕円曲線のときは因子類群と曲線自身が同型だったので, 各因子類は楕円曲線のある 1 点に対応していました. 種数が 2 以上のときは因子類の代表として, 曲線上の幾つかの点の組で表されます. 曲線上の有理点を幾つかとって, うまく組み合わせて適当な位数の有理因子類を作り出すのが彼のアイディアです.

$g \geq 1$ とする. 代数曲線

$$C : y^2 = f(x) = A^2(x) - \lambda\, x^{g+1}(x-a)^g$$

をとる. ここで $A(x) \in \mathbb{Q}[t]$ ($\deg A \leq g$), $\lambda \in \mathbb{Q}$ とし, $f(x)=0$ が重根を持たないようにとる. このとき C は種数 g の超楕円曲線で, $\mathbb{Q}$-有理点 $P_0=(0,\, A(0))$, $P_1=(1,\, A(1))$ をもつ. また $f(x)$ は奇数次なので C は唯一つの無限遠点 ∞ をもつ. このとき ∞ もまた $\mathbb{Q}$-有理的なので, $\{P_0,\, P_0',\, P_1,\, P_1',\, \infty\} \subset C(\mathbb{Q})$ となる. 因子 $D_0 = P_0 - \infty$, $D_1 = P_1 - \infty$ はともに $\mathbb{Q}$-有理因子なので, 因子類 $[D_0]$, $[D_1]$ は $\mathbb{Q}$-有理因子類になる.

命題 4.1　$a\,[D_0]+b\,[D_1]=0$ をみたす $a,\,b\in\mathbb{Z}$ をとり, $\ell=(g+1)\,b-g\,a$ とおく. このとき $\ell[D_0]=0$ が成り立つ.

この命題を示す. $\varphi(x,\,y)=y-A(x)\in\mathbb{Q}(C)$ とおくと,

$$\varphi\,\varphi'=(y-A(x))(-y-A(x))=-y^2+A^2(x)=\lambda\,x^{g+1}(x-1)^g$$

ここで $\varphi(P_0)=\varphi(P_1)=0$, $\varphi(P_0')\neq 0$, $\varphi(P_1')\neq 0$ なので,

$$\mathrm{div}(\varphi)=(g+1)\,P_0+g\,P_1-(2g+1)\,\infty=(g+1)\,D_0+g\,D_1$$

となる. 因子類で書くと $(g+1)\,[D_0]+g\,[D_1]=0$ となる. よって

$$\ell\,[D_0]=((g+1)b-g\,a)\,[D_0]=b(g+1)\,[D_0]-g\,a\,[D_0]=-b\,g\,[D_1]-g\,(-b)\,[D_1]=0$$

が従う.

(b)　Leprévost が最初に与えた 13 等分点をもつ種数 2 の超楕円曲線は, Flynn の方法を真似て作ったものであった. 有理的な Weierstrass 点で高々 22 位の極をもつ有理函数の全体の中で, 特定の零点をもつ有理函数を見つける必要があり, 煩雑な計算の後に得られている. 1992 年の位数 $2g^2+2g+1$ の有理等分点をもつ超楕円曲線は, $\ell=2g^2+2g+1=(g+1)^2+g^2$ $(a=-g,\,b=g+1)$ に対して上の命題を満たす $A(x)\in\mathbb{Q}[x]$, $\lambda\in\mathbb{Q}$ を与えたものである. 一般の g でも全く同じ計算で, ここでは $g=2$ で述べる. $2\times 2^2+2\times 2+1=13$ なので, 13 等分点をもつ種数 2 の超楕円曲線が得られる. 計算に必要な有理函数は, 有理的な Weierstrass 点で高々 5 位の極をもつもので, Flynn の方法の大幅な改良になっているだけでなく, 驚くほど簡単に定義方程式が得られる.

$a=-2$, $b=3$, $\ell=(2+1)\,b-2\,a=3^2+2^2=13$ とおく. $A(x)\in\mathbb{Q}[x]$ $(\deg A\le 2)$, $\lambda\in\mathbb{Q}$ で, 超楕円曲線 $C:y^2=f(x)=A^2(x)-\lambda\,x^3(x-1)^2$ の有理因子 $D_0=P_0-\infty$, $D_1=P_1-\infty$ が $-2[D_0]+3[D_1]=0$ となるものを与えたい. 超楕円対合で $D_0'=P_0'-\infty$ とおくと, $\mathrm{div}(x)=P_0+P_0'-2\infty$ なので, $[D_0']=-[D_0]$ となる. 満たすべき条件式は

$$0=-2[D_0]+3[D_1]=2[D_0']+3[D_1]=[2\,P_0'+3\,P_1-5\infty]$$

と書ける. 有理函数 h で $\mathrm{div}(h)=2\,P_0'+3\,P_1-5\infty$ となるものを作ればよい. ∞ でのみ 5 位の極をもつ有理函数の全体 $L(5\infty)$ を考える. Riemann-Roch の定理より $\dim L(5\infty)=\ell(5\infty)=5-2+1=4$ となる. 座標関数 x は ∞ でのみ 2 位の極をもち, y は ∞ でのみ 5 位の極をもつ. $L(5\infty)$ は 1, x, x^2, y を基底にもつ. $h\in L(5\infty)$ なので $h=u(x)-y$ $(\deg u\le 2)$ とおける.

$$\mathrm{div}(h\,h')=\mathrm{div}(h)+\mathrm{div}(h)'=2\,(P_0+P_0'-2\infty)+3\,(P_1+P_1'-2\infty)=\mathrm{div}(x^2(x-1)^3)$$

なので,

$$h\,h'=\mu\,x^2(x-1)^3\quad(\mu\in\overline{\mathbb{Q}})$$

と書ける.

$$h\,h'=(u(x)-y)(u(x)+y)=u^2(x)-y^2=u^2(x)-A^2(x)+\lambda\,x^3(x-1)^2$$

だから,

$$(u(x)-A(x))(u(x)+A(x))=u^2(x)-A^2(x)=x^2(x-1)^2((\mu-\lambda)x-\mu)$$

を得る. $A(x)$ も $u(x)$ も次数は 2 以下なので, $\mu=\lambda$ である. $h=u(x)-y$ は $P_0'=(0,\,-A(0))$ と $P_1=(1,\,A(1))$ を零点にもつので, $u(0)+A(0)=0$, $u(1)-A(1)=0$ を満たす. 従って

$$u(x)-A(x)=r\,(x-1)^2\ ,\ \ u(x)+A(x)=s\,x^2\ ,\ \ r\,s=-\lambda\quad(r,\,s\in\overline{\mathbb{Q}})$$

となる.

すべてを 1 パラメータつきで取り直して,

$$\lambda=4\,t\in\mathbb{Q}(t)\ ,\quad A(t)=t\,x^2-(x-1)^2,\ \ u(x)=t\,x^2+(x-1)^2\in\mathbb{Q}(t)[x]\quad(r=-2\ ,\ \ s=2t)$$

とおく. $\mathbb{Q}(t)$ 上定義された超楕円曲線

$$C:y^2=(t\,x^2-(x-1)^2)^2-4\,t\,x^3(x-1)^2$$

において, 有理函数 $y-u(x)$ の因子は $\mathrm{div}(y-u(x))=2\,P_0'+3\,P_1-5\infty$ である. $-2\,[D_0]+3\,[D_1]=0$ なので, 有理因子類 $[D_0]$ は $13\,[D_0]=0$ を満たす.