楕円曲線の有理点, 等分点, 同種写像 . . .
過去から現在へ
— 何が知られているか —

小川 裕之 (大阪大学大学院 理学研究科)

§1　楕円曲線論に関するノート

§1.1　Weierstrass 標準形, 判別式, j-不変量

K を体とする. 3 次代数曲線

$$E/K : y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6$$
$$a_1,\, a_2,\, a_3,\, a_4,\, a_6 \in K$$

この方程式を **Weierstrass 方程式**といい, 代数曲線 E/K の **Weierstrass 標準形** (**Weierstrass model**) という.

$$b_2 = a_1^2 - 4\,a_2, \quad b_4 = 2\,a_4 + a_1\,a_3, \quad b_6 = a_3^2 + 4\,a_6$$
$$b_8 = a_1^2\,a_6 + 4\,a_2\,a_6 - a_1\,a_3\,a_4 + a_2\,a_3^2 - a_4^2$$
$$c_4 = b_2^2 - 24\,b_4, \quad c_6 = -b_2^3 + 36\,b_2\,b_4 - 216\,b_6$$

とおく. K の標数が 2 でなければ E/K は

$$y^2 = 4\,x^3 + b_2\,x^2 + 2\,b_4\,x + b_6$$

に K 上同型である. さらに K の標数が 2 でも 3 でもなければ,

$$y^2 = x^3 - 27\,c_4\,x - 54\,c_6$$

に K 上同型である.

$$\Delta = -b_2^2\,b_8 - 8\,b_4^3 - 27\,b_6^2 + 9\,b_2\,b_4\,b_6 = (c_4^3 - c_6^2)/1728$$

Δ を 3 次代数曲線 E/K の (Weierstrass model の) **判別式**という. 判別式 Δ が消えていなければ ($\Delta \neq 0$) E は特異点を持たない. このとき E/K を K 上定義された**楕円曲線** (**an elliptic curve**) という. ここでは, 楕円曲線というときには $\Delta \neq 0$ を仮定する. 判別式が消えているとき, E は唯一つの特異点を持ち, その特異点は K 上有理的である. 3 次曲線の特異点は, 結節点 (**node**, $K \subset \mathbb{R}$ で描くなら曲線が自分自身と交差している点, 接線を 2 本もっている点) か単純尖点 (**cusp**, simple

1999 年 7 月 7 日版

cusp, $K \subset \mathbb{R}$ で描くなら曲線が折り返している点, 接線は唯一つ) のいずれかである. 非特異のとき, 楕円曲線 E/K に無限遠点 $O = [0:1:0]$ を零元とする群演算が定義され, K 上の 1 次元アーベル多様体の構造が入る. 実際その演算は次の様に定義される. E の点 P, Q をとる. 3 次曲線 E は, 直線 PQ と P, Q, R の 3 点で交わり, さらに 直線 OR と O, R, R' で交わる. $P+Q=R'$ で楕円曲線 E の上の演算 $+$ を定義する. (この演算により $(E, +)$ が K 上の可換代数群の構造をもつことを確めてみよ.) とくに P, Q が K-有理点なら作り方から R も K-有理点である. O も K-有理点だから, 結局 R' 即ち $P+Q$ も K-有理点である. 従って K-有理点の全体

$$E(K) = (E \text{ の } K \text{ 有理点の全体のなす集合})$$

はアーベル群をなし, 楕円曲線 E の **Mordell-Weil 群**と呼ばれる.

楕円曲線 E/K $(\Delta \neq 0)$ に対して

$$j = j(E) = c_4^3/\Delta$$

とおく. 楕円曲線 E/K の **j-不変量**という. $1728\,\Delta = c_4^3 - c_6^2$ だから

$$j = 1728\,\frac{c_4^3}{c_4^3 - c_6^2}$$

と書ける.

定理 1.1 体 K の代数閉包 $\overline{K}$ を固定する.

(1) j-不変量は, 楕円曲線の $\overline{K}$-同型不変量である. すなわち, 2 つの楕円曲線が代数的閉体 $\overline{K}$ 上同型であることと, j-不変量が等しいことは同値である.

(2) 任意の $j \in K$ に対して, j を j-不変量にもつ楕円曲線 E/K が存在する.

(3) E/K を楕円曲線, k を K に含まれる素体とする. $\overline{K}$-同型な E の *model* として $k(j(E))$ 上定義されたものがとれる.

この定理の (2) の楕円曲線の model として, $j \neq 0$, 1728 なら、

$$E : y^2 + x\,y = x^3 - \frac{36}{j - 1728}\,x - \frac{1}{j - 1728}$$

をとることができる (判別式, j-不変量などを計算してみよ). $j = 0$, 1728 については

$$\begin{aligned} y^2 + y &= x^3, \qquad \Delta = -27 \quad j = 0 \\ y^2 &= x^3 + x, \qquad \Delta = -64 \quad j = 1728 \end{aligned}$$

K の標数が 2 または 3 なら $0 = 1728$ であることに注意すれば以上ですべての標数, すべての j に対して $j(E) = j$ となる楕円曲線 E/K が与えられた. 同時に定理の (3) も確められている.

Weierstrass 標準形で定義された楕円曲線 E/K に対して

$$\omega = \frac{dx}{2\,y + a_1\,x + a_3}$$

とおく. ω は, 楕円曲線 E の加法に関して不変である $(\omega(P+Q) = \omega(P))$. 楕円曲線 E/K の**不変微分** (**the invariant differential, the Néron differential**) と呼ばれる.

§1.2 同種写像, 準同型環

楕円曲線間の非定数射

$$\lambda : E \to E', \qquad \lambda(O) = O$$

を, **同種写像** (**an isogeny**) という. 同種写像 λ は群準同型射である. 恒等的に O に写す射を O 写像 (あるいは単に O) と書き, O 写像もまた同種写像に含めて考えることもある. O でない同種写像 λ は, 全射で, 核 $\ker\lambda$ は E の有限部分群である. 曲線の有限射としての射 λ の次数のことを, 同種写像 λ の次数 $\deg\lambda$ という. O 写像の次数は, 0 と定める. 楕円曲線 E から E' へ O でない同種写像があるとき, E と E' は**同種** (**isogenous**) であるといい $E \sim E'$ と書く. 同種 "$\sim$" は同値関係をなす.

自分自身への同種写像 (自己準同型写像という) の全体の集合 $\mathrm{End}(E)$ は, 写像の和, 合成に関して環をなす. **準同型環**という. E の各点を m-倍する写像 ($[m]$ と書く) は自己準同型で, 他の準同型と可換である. $m \mapsto [m]$ により $\mathbb{Z}$ は $\mathrm{End}(E)$ の部分環とみなせる.

次数 n の同種写像 $\lambda : E \to E'$ に対して,

$$\exists! \, \widehat{\lambda} : E' \to E : \text{同種} \quad \text{s.t.} \quad \widehat{\lambda} \circ \lambda = [n]_E, \quad \lambda \circ \widehat{\lambda} = [n]_{E'}$$

この $\widehat{\lambda}$ を, 同種写像 λ の**双対同種写像** (**the dual isogeny**) という. 次の事実は基本的である.

$$\widehat{\widehat{\lambda}} = \lambda, \qquad \widehat{\lambda+\mu} = \widehat{\lambda} + \widehat{\mu}, \qquad \widehat{\lambda\circ\mu} = \widehat{\mu} \circ \widehat{\lambda}, \qquad \widehat{[m]} = [m]$$

$\lambda \mapsto \widehat{\lambda}$ は $\mathrm{End}(E)$ の anti-involution を与える. 次節で Tate 加群を使って得られることだが, $\mathrm{End}(E)$ は $\mathbb{Z}$-加群として階数は高々 4 である. 準同型環についてより詳しく,

定理 1.2 (Deuring) 楕円曲線 E/K の準同型環 $\mathrm{End}(E)$ は,
(1) 有理整数環 $\mathbb{Z}$,
(2) 虚 2 次体の整環,
(3) 4 元数環の極大整環
のいずれかに $\mathbb{Z}$ 上の多元環として同型である. ただし, 最後のもの (3) が現れるのは K の標数が正の場合に限り, K が有限体なら (1) は現れない.

楕円曲線 E が $\mathbb{Z}$ より真に大きい準同型環をもつとき, E は**虚数乗法**を持つ (**CM 型**) という. そうでないとき **non-CM 型**という. さらに 4 元数環の極大整環となるとき, E を**超特異 (supersingular)** 楕円曲線という.

§1.3 等分点, Tate 加群, ℓ-進表現

楕円曲線 E/K について, m-倍写像 $[m]$ で消える E の点を m-**等分点**といい, その全体を $E[m]$ $(= \ker[m])$ と書く. 楕円曲線の等分点は K 上代数的である. つまり, どの $m > 0$ に対しても $E[m] \subset E(\overline{K})$. $\mathrm{End}(E)$ のイデアル I に対しても同様に, I のすべての元で消える E の点を I-等分点といい, その全体を $E[I]$ と書く. E の自己準同型 λ に対して, $E[\lambda] = E[(\lambda)]$ である. E の等分点の全体を E_{tors} とおくと, $E_{\mathrm{tors}} = \cup_{m\geq 1} E[m]$ と書くことができる.

命題 1.3 (a) K の標数 p が 0 であるか, $p \nmid m$ であるなら,

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

(b) K の標数 p が正のとき,

$$E[p^r] \simeq \mathbb{Z}/p^r\mathbb{Z} \text{ or } O$$

p-等分点がすべて消えている ($E[p] = O$) とき, E を**超特異** (**supersingular**) **楕円曲線**という. 前節の最後に準同型環の構造で同じ言葉 "超特異" を定義したが, これらは矛盾していないことを後の節で見る.

ℓ を素数とする. ℓ-巾等分点の群と ℓ-倍写像 $[\ell] : E[\ell^{r+1}] \to E[\ell^r]$ からなる射影系について, その射影極限

$$T_\ell(E) = \varprojlim E[\ell^r]$$

を, E の **Tate 加群**という. Tate 加群は, 自由 $\mathbb{Z}_\ell$-加群で, K の標数が ℓ と異なるなら階数は 2 である.

$$V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

とおく. V_ℓ もまた Tate 加群と呼ばれる.

K は完全体であると仮定し, K の代数閉包 $\overline{K}$ を固定する. Galois 群 $\mathrm{G}_K = \mathrm{Gal}(\overline{K}/K)$ は自然に m-等分点 $E[m]$ に作用する.

$$\overline{\rho}_m : \mathrm{G}_K \longrightarrow \mathrm{Aut}(E[m])$$

この作用は射影系 $\{[\ell] : E[\ell^{r+1}] \to E[\ell^r]\}$ と可換だから, Tate 加群 $T_\ell(E)$, $V_\ell(E)$ への作用にのびる.

$$\rho_\ell : \mathrm{G}_K \longrightarrow \mathrm{Aut}(T_\ell(E)), \qquad \rho_\ell : \mathrm{G}_K \longrightarrow \mathrm{Aut}(V_\ell(E))$$

位相を考えた上での連続性はここでは省略する. 詳細は Serre : "Abelian ℓ-adic repersentations and elliptic curves" を参照のこと.

定理 1.4 (Serre) 代数体 K 上定義された楕円曲線 E が虚数乗法をもたないとき,

(a) すべての素数 ℓ について, ρ_ℓ の像は $\mathrm{Aut}(T_\ell(E))$ で有限指数である.

(b) 有限個の素数を除くすべての素数 ℓ について, ρ_ℓ の像は $\mathrm{Aut}(T_\ell(E))$ に一致する.

楕円曲線の間の同種写像 $\lambda : E \to E'$ は m-等分点を m-等分点にうつすから, $\mathbb{Z}_\ell$-線形写像 $\lambda_\ell : T_\ell(E) \to T_\ell(E')$ を引き起こす.

定理 1.5 自然な写像

$$\mathrm{Hom}(E, E') \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}(T_\ell(E), T_\ell(E'))$$

は単射である. 従って $\mathrm{Hom}(E, E')$ は $\mathbb{Z}$ 上階数が高々 4 の自由加群である.

λ も K 上定義されているなら, $\lambda_\ell : T_\ell(E) \to T_\ell(E')$ は Galois 加群の Galois 不変な準同型を与える.

定理 1.6 (Tate, Faltings) K が有限体 *(Tate)* か, 代数体 *(Faltings)* のとき,

$$\mathrm{Hom}_K(E, E') \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}(T_\ell(E), T_\ell(E'))^{\mathrm{G}_K}$$

§1.4 Weil pairing

E/K を楕円曲線, $m > 1$ を整数とする. K の標数は 0 であるか, m を割っていないと仮定する. $S, T \in E[m]$ とする. 代数曲線 E の因子 (divisor, E の点を生成元とする $\mathbb{Z}$-係数の有限形式和)

$$\sum_{[m]T'=T} (T') - \sum_{[m]R=O} (R)$$

は 0 に線形同値である (E 上の関数の零点, 極から作った因子として表される). このことは, 因子としての和, 差を楕円曲線の演算と思って計算してみればすぐにわかる. 本来楕円曲線の加法は, E の点 P, Q に対して $(P) + (Q) - (X) - (O)$ が 0 に線形同値となるような E の点 X をとり $P + Q = X$ と定義される. §1.1 ではこの E の点 X を見つける手順で演算を定義したのであった. さて話を元に戻して, 上で考えた因子を零点, 極にもつ関数 g をとる. E の点 X を任意にとって,

$$e_m(S, T) = \frac{g(X+S)}{g(X)}$$

命題 1.7 (Weil pairing) (a) $e_m(S, T)$ の定義の右辺は X のとり方に依らず S, T のみに依る.
(b) $e_m(S, T)$ の値は *1* の m-乗根で

$$e_m : E[m] \times E[m] \longrightarrow \mu_m$$

は双線形, 交代的, 非退化な *pairing* で, *Galois* 群の作用と可換である. *(i.e.* $e_m(S^\sigma, T^\sigma) = e_m(S, T)^\sigma$ *(for* $^\forall \sigma \in \mathrm{G}_K$*))*

この pairing e_m を **Weil pairing** という. Weil pairing の性質を使った最初の重要な事実として,

系 1.8 K 上定義された楕円曲線の m-等分点がすべて K 上有理的ならば, K は *1* の m-乗根をすべて含む.

系 1.9 $E/\mathbb{Q}$ を楕円曲線とする. 奇素数 p に対して $E(\mathbb{Q})_{\mathrm{tors}}$ の p-部分の階数は高々 *1* である. $E(\mathbb{Q})_{\mathrm{tors}}$ が有限なら, $E(\mathbb{Q})_{\mathrm{tors}}$ は巡回群か, $\mathbb{Z}/2\mathbb{Z}$ と巡回群の直積のいずれかに同型である.

命題 1.10 $\lambda : E \to E'$ を楕円曲線の間の同種写像, $S \in E[m]$, $T \in E'[m]$ とする. このとき,

$$e_m(S, \widehat{\lambda}(T)) = e_m(\lambda(S), T)$$

Weil pairing は Tate 加群の上の pairing にのばすことができる.

命題 1.11 双線形, 交代的, 非退化, *Galois* 群の作用と可換な *pairing* が存在する.

$$e_\ell : T_\ell(E) \times T_\ell(E) \longrightarrow T_\ell(\mu)$$

§1.5 有限体上の楕円曲線の zeta 関数

$E/\mathbb{F}_q$ を位数 q の有限体 $\mathbb{F}_q$ 上定義された楕円曲線とする. ϕ_q を E 上の **q-乗 Frobenius 準同型**とおく. Frobenius 準同型は, 点の座標を使って $\phi_q : E \ni (x, y) \mapsto (x^q, y^q) \in E$ と書ける. 明らかに $\deg \phi_q = q$ である. $a = a(E) = 1 - \sharp E(\mathbb{F}_q) + q$ とおく.

命題 1.12

$$\phi_q + \widehat{\phi}_q = [a]$$

$\phi_q \cdot \widehat{\phi_q} = [\deg \phi_q] = [q]$ だから, ϕ_q は $X^2 - a\,X + q$ を特性多項式にもつ.

定理 1.13 (Hasse)

$$|1 - \sharp E(\mathbb{F}_q) + q| \leq 2\sqrt{q}$$

$q = p$ が素数のとき, つまり楕円曲線 E が素体 $\mathbb{F}_p$ 上定義されているとき, Frobenius ϕ_p の特性多項式の判別式 $(a^2 - 4\,p)$ は, 定理より負の数である. 準同型環 $\mathrm{End}(E)$ の部分環 $\mathbb{Z}[\phi_p]$ は判別式 $a^2 - 4\,p$ の虚 2 次の整環になる. 有限素体上定義された楕円曲線は CM 型か supersingular であることを, このようにして確めるもできる. Frobenius を含む整環 $\mathbb{Z}[\phi_p]$ が極大整環で E が supersingular でない (ordinary という) なら $\mathrm{End}(E) = \mathbb{Z}[\phi_p]$ で準同型環が決まる. 素体上定義されているものについては, §1.7 で見る類多項式を使って, 準同型環を具体的に決めることができる (ordinary の場合は山本芳彦氏 (数理研講究録 759), supersingular の場合は私 (数理研講究録 775)).

形式的巾級数

$$Z(E/\mathbb{F}_q, T) = \exp\Big(\sum_{n=1}^{\infty} \sharp E(\mathbb{F}_{q^n})\,\frac{T^n}{n}\Big)$$

を $E/\mathbb{F}_q$ の **zeta 関数**という.

定理 1.14

$$Z(E/\mathbb{F}_q, T) = \frac{1 - a\,T + q\,T^2}{(1-T)\,(1-q\,T)}$$

さらに

$$1 - a\,T + q\,T^2 = (1 - \alpha\,T)\,(1 - \beta\,T), \quad |\alpha| = |\beta| = \sqrt{q}$$

定理 1.15 $\mathbb{F}_q$ 上定義された *2* つの楕円曲線 E, E' が $\mathbb{F}_q$ 上同種ならば, E, E' の $\mathbb{F}_q$-有理点の個数は同じである. 従って両者の *zeta* 関数は一致する.

$$Z(E/\mathbb{F}_q, T) = Z(E'/\mathbb{F}_q, T)$$

§1.6 局所体上の楕円曲線

K を正規付値 v をもつ局所体, $\mathcal{O}$ をその整数環, $\mathfrak{p}$ を極大イデアル, $k = \mathcal{O}/\mathfrak{p}$ を剰余体, その標数を p とする. E/K を楕円曲線とする. 係数が整数になるように Weierstrass 標準形をとる.

$$E : y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6 \quad (a_i \in \mathcal{O})$$

K 上の同型な $\mathcal{O}$-係数の model の中で判別式の付値 $v(\Delta)$ が最小になる model を, **極小 model** (**minimal Weierstrass model**) という. $\mathcal{O}$-係数の model の各係数を modulo $\mathfrak{p}$ で見ることにより, 剰余体 k に係数を持つ 3 次曲線が得られる. これを E の **reduction** (**reduction modulo** $\mathfrak{p}$) といい, $\tilde{E}$ と書く.

命題 1.16 $\mathfrak{p} \nmid \Delta$ のとき, *reduction* $\tilde{E}$ は非特異, つまり k 上の楕円曲線である. さらに

$$\mathrm{End}(E) \hookrightarrow \mathrm{End}(\tilde{E})$$

E が K 上非特異 ($\Delta \neq 0$) であっても, $\mathfrak{p} \,|\, \Delta$ ならば $\tilde{E}$ は特異点をもつことがわかる. $\tilde{E}$ が非特異 ($\mathfrak{p} \nmid \Delta$) のとき, E は **good** (or **stable**) **reduction** をもつという. $\tilde{E}$ が node をもつとき, E は **multiplicative** (or **semi-stable**) **reduction** をもつという. さらにその node での接線が k 上定義されるとき, E は **split multiplicative reduction** をもつといい, そうでないとき, E は **non-split multiplicative reduction** をもつという. $\tilde{E}$ が cusp をもつとき, E は **additive** (or **unstable**) **reduction** をもつという. 言葉だけの問題だが semi-stable と言うときには good も含めて言われることが多い.

K を代数体の場合, K 上定義された楕円曲線に対して, 各素イデアル $\mathfrak{p}$ について $\mathfrak{p}$-進完備体 $K_\mathfrak{p}$ 上の楕円曲線と見て reduction が定義でき, その型 (good など) についても同様に定義することができる.

命題 1.17 E/K を楕円曲線とする. 有限次拡大 K'/K が存在して, E を K' 上の楕円曲線と見たとき *reduction* の型が *good* か *split multiplicative* になるようにできる.

$\tilde{E}$ の非特異点の全体を $\tilde{E}^{\mathrm{ns}}$ とおく.

$$
\begin{aligned}
E^{(0)}(K) &= \{P \in E(K) \,|\, \tilde{P} \in \tilde{E}^{\mathrm{ns}}(k)\} \\
E^{(1)}(K) &= \{P \in E(K) \,|\, \tilde{P} = \tilde{O}\} \\
E^{(r)}(K) &= \{P \in E(K) \,|\, v(x(P)) \leq -2\,r\} \qquad (\text{for } r \geq 1)
\end{aligned}
$$

とおく. これは $E(K)$ の filtration を与える.

命題 1.18 (a)

$$0 \longrightarrow E^{(1)}(K) \longrightarrow E^{(0)}(K) \longrightarrow \tilde{E}^{\mathrm{ns}}(k) \longrightarrow 0$$

(b) $r \geq 1$ に対して, 座標関数 $x : P \mapsto x(P)$ は, 単射準同型

$$E^{(r)}(K)/E^{(r+1)}(K) \longrightarrow \mathfrak{p}^{2r}/\mathfrak{p}^{2r+2}$$

を引き起こす.

定理 1.19 (Kodaira-Néron) $E(K)/E^{(0)}(K)$ は有限である. さらに *split multiplicative reduction* でないなら, その位数は高々 *4* で, *split multiplicative reduction* なら, 位数 $v(\Delta)$ の巡回群である.

系 1.20 E が *good reduction* をもち, m が剰余体 k の標数 p と素なとき, *reduction map* の K-有理 m-等分点への制限 $E(K)[m] \to \tilde{E}(k)$ は, 単射である.

系 1.21 拡大 $K(E[m])/K$ は, 不分岐である.

Galois 加群が不分岐であるとは, 惰性群 (the inertia subgroup) の作用が自明であるときを言う.

定理 1.22 (Néron-Ogg-Shafarevich の criterion) 次は同値である.

(1) E は *good reduction* をもつ.
(2) p と素な無数に多くの m に対して, $E[m]$ は不分岐である.
(2') p と素なすべての m に対して, $E[m]$ は不分岐である.
(3) ある素数 $\ell \neq p$ で $T_\ell(E)$ が不分岐なものが存在する.
(3') すべての素数 $\ell \neq p$ に対して, $T_\ell(E)$ は不分岐である.

系 1.23 *K 上定義された K 上同種な 2 つの楕円曲線の reduction の型は, ともに good であるかともに good でないかのいずれかである.*

楕円曲線 E/K が potentially good reduction をもつとは, 適当な有限次拡大 K'/K で E/K' が good reduction をもつときを言う.

命題 1.24 *E/K が potentially good reduction をもつことは, $j(E) \in \mathcal{O}$ であることと同値である.*

§1.7 Supersingular 楕円曲線

K を標数 $p > 0$ の完全体, E/K を楕円曲線とする. $\phi : E \to E^{(p)}$ を p-乗 Frobenius 写像, $\widehat{\phi} : E^{(p)} \to E$ をその dual とする.

命題 1.25 *p-倍写像 $[p]$ が純非分離的ならば, $j(E) \in \mathbb{F}_{p^2}$ である.*

定理 1.26 (Deuring) 次は同値である.
(i) $E[p] = O$
(ii) $\widehat{\phi}$ は純非分離的.
(iii) p-倍写像 $[p]$ は純非分離的.
(iv) E の準同型環 $\mathrm{End}(E)$ は非可換.

楕円曲線 E/K がこの定理の条件 (i) $\sim$ (iv) を満たすとき (§1.2 の最後で定義したのと同じことだが), **超特異** (**supersingular** あるいは単に **s.s.**) といい, そうでないものを**通常** (**ordinary**) という. 前の命題とあわせると

系 1.27 *supersingular 楕円曲線は $\mathbb{F}_{p^2}$ 上定義された model をもつ. 特に, supersingular 楕円曲線の同型類の個数は有限である.*

定理 1.28 (Deuring) *p を素数とする. p と ∞ のみ分岐する $\mathbb{Q}$ 上の正定値 4 元数環を $\mathbb{Q}_{p,\infty}$ とおく. $\overline{\mathbb{F}_p}$ 上定義された supersingular 楕円曲線の準同型環は, $\mathbb{Q}_{p,\infty}$ のある極大整環に環として同型である.*

定理 1.29 (Deuring) *$\mathcal{O}$ を $\mathbb{Q}_{p,\infty}$ の極大整環のひとつとする. $\overline{\mathbb{F}_p}$ 上定義された supersingular 楕円曲線の $\overline{\mathbb{F}_p}$-同型類は, 左 $\mathcal{O}$-イデアル類と 1 対 1 に対応する.*

定理 1.30 (Eichler) *$\mathbb{Q}_{p,\infty}$ の極大整環の類数 (左イデアル類の個数) を H とおくと, H は有限で,*

$$H = \frac{p-1}{12} + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right) + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right)$$

定理 1.31 *$\mathbb{F}_p$ 上定義された supersingular 楕円曲線の $\overline{\mathbb{F}_p}$-同型類の個数は,*

$$\frac{h(-p) + h(-4p)}{2}$$

である. ただし, $h(D)$ は判別式 D の 2 次の整環 $\mathbb{Z}[\dfrac{D+\sqrt{D}}{2}]$ の類数で, $D \not\equiv 0, 1 \pmod 4$ のときは 0 とおく.

一方 ordinary については

定理 1.32 K を標数 $p>0$ の体, E/K を *ordinary* 楕円曲線とする.
(a) $j(E)\in\overline{\mathbb{F}_p}$ なら $\mathrm{End}(E)$ は虚 2 次体の整環.
(b) $j(E)$ が素体 $\mathbb{F}_p$ 上超越的なら $\mathrm{End}(E)\simeq\mathbb{Z}$ である.

定理 1.33 (Deuring の持ち上げ定理) $\overline{E}/\mathbb{F}_q$ を楕円曲線, $\overline{\lambda}\in\mathrm{End}(\overline{E})-\mathbb{Z}$ を任意にとり固定する. 有限次代数体 K と素イデアル $\mathfrak{p}$, $\mathfrak{p}$ で *good reduction* をもつ *CM* 型楕円曲線 E/K, $\lambda\in\mathrm{End}(E)$ で $\overline{E}=\widetilde{E}$, $\overline{\lambda}=\widetilde{\lambda}$ をみたすものが存在する.

$D<0$, $D\equiv 0,1\pmod 4$ に対して, $\mathcal{O}_D=\mathbb{Z}[\dfrac{D+\sqrt{D}}{2}]$ を判別式 D の虚 2 次の整環, $h(D)$ をその類数とする.

$$P_D(X)=\prod_E (X-j(E))$$

ただし, 積は $\mathrm{End}(E)\simeq\mathcal{O}_D$ なる楕円曲線 $E/\mathbb{C}$ の $\mathbb{C}$-同型類の代表系をわたるものとする. $P_D(X)$ を (**判別式 D の**) **類多項式** (**class polynomial**) という. 虚数乗法論より

命題 1.34 $P_D(X)$ は $h(D)$ 次の $\mathbb{Z}$-係数, *monic,* 既約, アーベル多項式である.

類多項式 $P_D(X)$ は $-3\geq D\geq -1500$ について具体的に計算されたデータがある (Kaneko, Yamamoto など). また楕円曲線暗号の理論において効率性, 安全性の検証に重要な役割を演ずることから, とてつもなく大きな類数をもつ虚 2 次の整環のとてつもなく大きな判別式に対して, 類多項式が計算されている. j-関数 $j(\tau)$ の Fourier 展開を使って j-不変量の近似値を求め, 類多項式の係数の近似値を求める. 上の命題よりその係数は整数だから, 誤差を評価して十分に整数に近いところまで近似の精度をあげれば, 類多項式を具体的に計算することができる. やってみればわかることだが, 類多項式の係数は類数あるいは判別式に比べて非常に大きい. 2 つの類多項式 $P_{D_1}(X)$ と $P_{D_2}(X)$ (D_1, D_2 は異なる虚 2 次体に属する判別式) の終結式の素因数分解には小さな素因子しか現れていない. Gross-Zagier (J. reine. angew. Math. 355 (1985), 191–220) は, このことの説明のひとつとして終結式を計算する公式を与えた. 多くの既知の類多項式を使い, それらとの終結式を Gross-Zagier の公式で計算すれば, 代数的に連立方程式を解く形で未知の類多項式を計算することができる. 例えば類数 1 の 9 つの虚 2 次の極大整環 (判別式は -3, -4, -7, -8, -11, -19, -43, -67, -163) の類多項式 (これらは既知とする) との終結式を計算することで, 類数が 9 以下の虚 2 次の整環の類多項式が計算できる. この方法は代数的な計算しか使っていない. 多少とも曖昧さをもつ近似計算は使わないので, 数学的には改善された手順と言えるかもしれないが, 技術的には (計算量の面からは) 改善されているわけではない.

類多項式 $P_D(X)$ を有限体 $\mathbb{F}_q$-係数の多項式と思うことができる. 類多項式で Deuring の持ち上げ定理を言いかえると

定理 1.35 (Deuring) 楕円曲線 $E/\mathbb{F}_q$ とする.
(i) 埋め込み $\mathcal{O}_{D'}\hookrightarrow\mathrm{End}(E)$ が存在するなら, $D'=c^2\,D$ なる D で $P_D(j(E))=0$ なるものがとれる.
(ii) $P_D(j(E))=0$ ならば埋め込み $\mathcal{O}_D\hookrightarrow\mathrm{End}(E)$ が存在する.

ordinary と supersingular との違いが見えてくる. ordinary の場合, $\mathrm{End}(E)$ 自身が虚 2 の整環なので $P_D(j(E))=0$ なる D はひとつの虚 2 次体に属する判別式に限るが, supersingular の場合, 様々な虚 2 次の整環の $\mathrm{End}(E)$ への埋め込みがあるので, $P_D(j(E))=0$ なる判別式 D として多様な虚 2 次の整環の判別式が現れる.

定理 1.36 (Kaneko (Osaka J. Math. 26 (1989), no. 4, 849–855)) $E/\mathbb{F}_p$ が *supersingular* 楕円曲線とする. $D \leq \frac{4}{\sqrt{3}}\sqrt{p}$ で $P_D(j(E)) = 0$ なるものが存在する.

定理 1.37 (Kaneko) *2* つの判別式 D_1, D_2 が $D_1 D_2 < 4p$ をみたすとき, $P_{D_1}(X) \bmod p$ と $P_{D_2}(X) \bmod p$ は 共通根をもたない. 言いかえると, $P_{D_1}(X)$ と $P_{D_2}(X)$ の終結式の素因子 p は $p \leq \dfrac{D_1 D_2}{4}$ をみたす.

定理 1.38 (Elkies) $p \equiv 3 \pmod 4$ を素数とする. 次をみたす多項式 $R(X)$, $S(X) \in \mathbb{Z}[X]$ が存在する.

$$P_p(X) \equiv (X - 1728)\,(R(X))^2 \bmod p$$
$$P_{4p}(X) \equiv (X - 1728)\,(S(X))^2 \bmod p$$

定理 1.39 (Kaneko) p を素数とする.
(1) $p \equiv 1 \pmod 4$ のとき, $P_p(X) \bmod p$ は多項式の平方.
(2) $p \equiv 3 \pmod 4$ のとき, $P_p(X)\,P_{4p}(X) \bmod p$ は多項式の平方.

楕円曲線 $E/\mathbb{Q}$ に対して, $\widetilde{E}/\mathbb{F}_p$ reduction modulo p が supersinguler になる素数 p (supersinguler prime という) の密度に関する予想がある. $x > 0$ に対して,

$$\pi_E(x) = \sharp\{p < x \,|\, \widetilde{E}/\mathbb{F}_p \text{ は supersingular}\}$$

とおく.

定理 1.40 (Deuring) E が *CM* 型 *(*虚数乗法をもつ*)* ならば,

$$\pi_E(x) \sim \frac{1}{2}\,\pi(x)$$

予想 1.41 (Lang-Trotter) $E/\mathbb{Q}$ が *non-CM* 型なら, E のみに依存する定数 C_E が存在して,

$$\pi_E(x) \sim C_E\,\sqrt{x}/\log x$$

$E/\mathbb{Q}$ は non-CM 型とする. (以下の内容に関する詳細は, 数理研講究録 821 の金子昌信氏の解説を参考にして下さい.) $\pi_E(x)$ について下から評価するのは非常に難しく,

定理 1.42 (Brown (Bull. London Math. 20 (1988))) 一般 *Riemann* 予想のもとで

$$\pi_E(x) \gg \log\log\log x$$

定理 1.43 (Elkies (Invent. Math. 89 (1987), no. 3, 561–567))

$$\pi_E(x) \longrightarrow \infty \quad as\ x \to \infty$$

一方, 上からの評価は色々あるが, 一般 Riemann 予想を仮定しない次のものが現在最良の評価である.

定理 1.44 (Elkies (Astérisque No. 198-200 (1991), 127–132 (1992)))

$$\pi_E(x) = O(x^{3/4})$$

§1.8 Lutz-Nagell の定理, Bergman の定理, Cassels の定理

K を正規付値 v をもつ標数 0 の局所体, $\mathcal{O}$ を整数環, k を剰余体とする. さらに剰余体 k の標数 p は正であると仮定する. E/K を $\mathcal{O}$-係数の Weierstrass 標準形で与えられた楕円曲線とする. §1.6 で与えた $E(K)$ の filtration を $\{E^{(r)}(K)\}_r$ と書く.

定理 1.45 (Cassels) (1) p と素な m に対して

$$E(K)[m] \cap E^{(1)}(K) = O$$

(2) 正の整数 e に対して $r_e = \left[\dfrac{v(p)}{p^e - p^{e-1}}\right]$ とおく. このとき,

$$E(K)[p^e] \cap E^{(r_e+1)}(K) = O$$

K を有限次代数体, $\mathcal{O}$ をその整数環とする. E/K を $\mathcal{O}$-係数の Weierstrass 標準形で定義された楕円曲線とする. K の各有限素点 v に関する完備体 K_v について, E を K_v 上の楕円曲線と見たときの $E(K_v)$ の filtration を $\{E_v^{(r)}(K_v)\}_r$ とする. このとき, 上の Cassels の定理より次が従う.

定理 1.46 p を素数, e を正の整数とする. $r = \left[\dfrac{v(p)}{p^e - p^{e-1}}\right]$ とおくとき,

$$E(K)[p^e] \cap E_v^{(r+1)}(K_v) = O$$

特に $\mathfrak{p}_v \nmid p$ ならば K-有理 p-巾等分点は $\mathfrak{p}_v$-*integral.*

$K = \mathbb{Q}$ とする.

系 1.47 奇素数 p に対して $E(\mathbb{Q})_{\mathrm{tors}} \cap E_p^{(1)}(\mathbb{Q}_p) = O$. $E(\mathbb{Q})_{\mathrm{tors}} \cap E_2^{(2)}(\mathbb{Q}_2) = O$.

系 1.48 楕円曲線 $E/\mathbb{Q}$ が素数 p で *good reduction* をもつとする. *reduction map* の $E(\mathbb{Q})_{\mathrm{tors}}$ への制限 $E(\mathbb{Q})_{\mathrm{tors}} \to \tilde{E}(\mathbb{F}_p)$ は, p が奇素数なら単射で, $p = 2$ ならその核は位数が高々 *2* である.

系 1.49 楕円曲線 $E/\mathbb{Q}$ に対して, $E(\mathbb{Q})_{\mathrm{tors}}$ は有限群である. さらに詳しく, 奇素数 p で *good reduction* をもつなら, $\sharp E(\mathbb{Q})_{\mathrm{tors}} \leq 1 + 2\sqrt{p} + p$. *2* で *good reduction* をもつなら, $\sharp E(\mathbb{Q})_{\mathrm{tors}} \leq 10$.

Weil pairing の節で "$E(\mathbb{Q})_{\mathrm{tors}}$ は位数有限" という仮定付きで述べられていたことだが, その仮定が常に満たされることがわかったので, 結局

系 1.50 楕円曲線 $E/\mathbb{Q}$ の $\mathbb{Q}$-有理等分点の全体は, 巡回群か, $\mathbb{Z}/2\mathbb{Z}$ と巡回群の直積に同型である.

与えられた楕円曲線に対して, 有理等分点を具体的に決めるには次の形の定理が使いやすい.

定理 1.51 (Lutz-Nagell) 楕円曲線 $E/\mathbb{Q} : y^2 = x^3 - a\,x - b$ *(*$a, b \in \mathbb{Z}$*)* について, $\Delta' = 4\,a^3 - 27\,b^2$ とおく *(model* の判別式は $\Delta = 16\,\Delta'$*)*. $P = (x_0, y_0) \in E(\mathbb{Q})_{\mathrm{tors}}$ とするとき,
(1) x_0, y_0 は整数である.
(2) $y_0 \neq 0$ ならば $y_0^2 \mid \Delta'$.

Billing (Nova Acta Soc. Sci. Upsaliensis (4) 11, no. 1 (1938)) は, 2 次体の場合に Lutz-Nagell の定理の拡張を与えた. しかし Bergman (Ark. Mat. 2, (1952). 299–305, Ark. Mat. 2, (1954). 489–535) によると Billing の証明には少々難があるそうで, 一般の有限次代数体への拡張を与え, その系として Lutz-Nagell の定理も含めて, 2 次体, 3 次体の場合に Lutz-Nagell の定理の statement がそのまま成立つことを示した. 上で最初に述べた Cassels の定理は, 次の Bergman の定理を定義方程式の形に依らないものにし更に多少の精密化を行ったものとなっている.

定理 1.52 (Bergman) K を有限次代数体とする. 楕円曲線 $E/K : y^2 = x^3 - a\,x - b$ *(*a, $b \in \mathbb{Z}$*)* について $\Delta' = 4\,a^3 - 27\,b^2$ とおく. $P = (x_0, y_0) \in E(K)_{\mathrm{tors}}$ とするとき,

(1) 次の何れかが成立するなら, 等分点 P の座標 x_0, y_0 は K の整数である.

[1] P の位数 n は奇素数の巾ではない.

[2] n は *3* の巾で, *3* は K の素イデアルの *8* 乗ではわれない.

[3] n は *3* より大きい素数で, n は K の素イデアルの $n-1$ 乗ではわれない.

また, n が奇素数 p の巾のとき, $p\,x_0$ はいつでも K の整数である.

(2) $n > 2$ で, P の x-座標 x_0 も P の *2*-倍点の x-座標 $x(2\,P)$ もともに K の整数なら, y_0 もまた K の整数で $y_0^2 \,|\, \Delta'$.

系 1.53 (Billing, Bergman) *2* 次または *3* 次の代数体 K 上の楕円曲線 $E/K : y^2 = x^3 - a\,x - b$ について, *Lutz-Nagell* の定理と同じ主張がなりたつ. すなわち, $\Delta' = 4\,a^3 - 27\,b^2$, $P = (x_0, y_0) \in E(K)_{\mathrm{tors}}$ とするとき,

(1) x_0, y_0 は K の整数である.

(2) $y_0 \neq 0$ ならば $y_0^2 \,|\, \Delta'$.

§1.9 Weak Mordell-Weil の定理, Selmer 群, Shafarevich-Tate 群, Descent Procedures

定理 1.54 (Mordell-Weil) K を素体上有限生成な体, E/K を楕円曲線とする. このとき, $E(K)$ は有限生成アーベル群をなす.

Mordell-Weil の定理の証明は, 2 つのステップに分けられる. 最初のステップは

定理 1.55 (weak Mordell-Weil Theorem) $E(K)/mE(K)$ は有限アーベル群.

を示すことで, descent と呼ばれる手続きから得られることをこの節で述べる. 次のステップでは, height 関数について話をし, その height による評価から目的の $E(K)$ が有限生成であることを示す. これは次節で見ることにする. 印象的に書くなら,

$$(\text{descent procedure}) + (\text{height}) \longrightarrow \text{Mordell-Weil}$$

といったところか...

K を完全体, E/K を楕円曲線とする. 整数 $m \geq 2$ に対して, Galois 加群の完全列

$$0 \longrightarrow E[m] \longrightarrow E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \longrightarrow 0$$

を考える. 長完全列をとると,

$$\begin{aligned} 0 \longrightarrow \quad E(K)[m] \quad &\longrightarrow \quad E(K) \quad \xrightarrow{[m]} \quad E(K) \\ \xrightarrow{\delta} H^1(\mathrm{G}_K,\, E[m]) &\longrightarrow H^1(\mathrm{G}_K,\, E(\overline{K})) \xrightarrow{[m]} H^1(\mathrm{G}_K,\, E(\overline{K})) \longrightarrow \end{aligned}$$

従って

$$0 \longrightarrow E(K)/mE(K) \xrightarrow{\delta} H^1(\mathrm{G}_K,\, E[m]) \longrightarrow H^1(\mathrm{G}_K,\, E(\overline{K}))[m] \longrightarrow 0$$

が得られる. この完全列を **(**m**-)Kummer 列** という. 写像 δ は, 長完全列の連結準同型 δ からくるもので, それは次の様にして定義される. $P \in E(K)$ に対して, $[m]\,Q = P$ なる $Q \in E(\overline{K})$ をとる. $\kappa(P,\, Q,\, \sigma) = Q^\sigma - Q$ $(\sigma \in \mathrm{G}_K)$ とおく. 1-cocycle $\kappa(P,\, Q,\, \sigma)$ は m-倍写像 $[m]$ で消える.

$\kappa(P, Q, \cdot) \in Z^1(\mathrm{G}_K, E[m])$). $\kappa(P, Q, \cdot)$ の属する 1-cohomology class を $\delta(P) \in H^1(\mathrm{G}_K, E[m])$ とおくと, $\delta(P)$ は Q のとり方によらない. 連結準同型 $\delta : E(K) \ni P \mapsto \delta(P) \in H^1(\mathrm{G}_K, E[m])$ が定義された.

すべての m-等分点が K 上有理的, すなわち $E[m] \subset E(K)$ と仮定する. $H^1(\mathrm{G}_K, E[m]) = \mathrm{Hom}(\mathrm{G}_K, E[m])$ となる. またこの場合上で与えた $\kappa(P, Q, \sigma)$ は Q の選び方に依らないので, 単に $\kappa(P, \sigma)$ と書くとこの $\kappa(;\dot{})$ は双線形な pairing

$$\kappa : E(K) \times \mathrm{G}_K \longrightarrow E[m]$$

と思うことができる. **Kummer pairing** という. $L_m = K([m]^{-1}E(K))$ とおく.

命題 1.56 (1) $\ker\{E(K) \ni P \mapsto \kappa(P, \cdot) \in \mathrm{Hom}(\mathrm{G}_K, E[m])\} = mE(K)$.

(2) $\ker\{\mathrm{G}_K \ni \sigma \mapsto \kappa(\cdot, \sigma) \in \mathrm{Hom}(E(K), E[m])\} = \mathrm{G}_{L_m}$.

従って,

$$\kappa : E(K)/mE(K) \times \mathrm{Gal}(L_m/K) \longrightarrow E[m]$$

もし $H^1(\mathrm{G}_K, E[m])$ が有限であったなら, Kummer 列から $E(K)/mE(K)$ が有限であることがわかるのだが, 実際そうはいかない. 例えばすべての m-等分点が K 上有理的の場合, $H^1(\mathrm{G}_K, E[m]) = \mathrm{Hom}(\mathrm{G}_K, E[m])$. 従って Galois 理論により, $H^1(\mathrm{G}_K, E[m])$ は, 有限アーベル群 $E[m]$ の部分群を Galois 群にもつアーベル拡大 L/K の全体に 1 対 1 に対応する. ここで主として扱いたい有限次代数体 K に対してこのような拡大体 L/K は無数に存在するから, 結局 $H^1(\mathrm{G}_K, E[m])$ は位数が有限ではい. $H^1(\mathrm{G}_K, E[m])$ を見ただけでは $E(K)/mE(K)$ を評価することはできない.

K を代数体, E/K を楕円曲線とする. E/K に関する m-Kummer 列と, K の素点 v に関する完備体 K_v 上の楕円曲線としての E/K_v に関する m-Kummer 列を, 自然な埋め込み $K \hookrightarrow K_v$ でつないで, 次の可換図式を考えることができる.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/mE(K) & \xrightarrow{\delta} & H^1(\mathrm{G}_K, E[m]) & \longrightarrow & H^1(\mathrm{G}_K, E(\overline{K}))[m] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_v E(K_v)/mE(K_v) & \xrightarrow{\delta_v} & \prod_v H^1(\mathrm{G}_{K_v}, E[m]) & \longrightarrow & \prod_v H^1(\mathrm{G}_{K_v}, E(\overline{K_v}))[m] & \longrightarrow & 0
\end{array}$$

くどいようだが, 先ほど $H^1(\mathrm{G}_K, E[m])$ を評価するだけで $E(K)/mE(K)$ の有限性を導こうとして失敗した. この可換図式を見ると, δ による $E(K)/mE(K)$ の像は $H^1(\mathrm{G}_K, E[m])$ の中でずっと小さそうであることがわかる. この可換図式によると $E(K)/mE(K)$ は $\prod_v E(K_v)/mE(K_v)$ から下の完全列を通って $\prod_v H^1(\mathrm{G}_{K_v}, E(\overline{K_v}))[m]$ で消えるから, δ の像は, $H^1(\mathrm{G}_K, E[m]) \to \prod_v H^1(\mathrm{G}_{K_v}, E(\overline{K_v}))[m]$ で消える部分に含まれる. そこで

$$S^{(m)}(E/K) = \ker\left\{H^1(\mathrm{G}_K, E[m]) \longrightarrow \prod_v H^1(\mathrm{G}_{K_v}, E(\overline{K_v}))[m]\right\}$$

とおく. **Selmer 群**という. さらに,

$$Ш(E/K)[m] = \ker\left\{H^1(\mathrm{G}_K, E(\overline{K}))[m] \longrightarrow \prod_v H^1(\mathrm{G}_{K_v}, E(\overline{K_v}))[m]\right\}$$

とおく. **Shafarevich-Tate 群** (の m-part) という.

命題 1.57

$$0 \longrightarrow E(K)/mE(K) \longrightarrow S^{(m)}(E/K) \longrightarrow Ш(E/K)[m] \longrightarrow 0$$

この完全列を **(m-)descent 列**という．目的の $E(K)/mE(K)$ の有限性は, Selmer 群の有限性に帰着された.

定理 1.58 K を有限次代数体, E/K を楕円曲線とする．m-等分点はすべて K-有理的とする．S を E の *bad prime* と m を割る素点の集合とし, $x \in H^1(\mathrm{G}_K, E[m])$ に対して $L_x = \overline{K}^{\ker x}$ とおく.

(a) L_x/K は高々 m^2 次のアーベル拡大である.

(b) $x \in S^{(m)}(E/K)$ ならば L_x/K は S の外で不分岐である.

(c) 特に *Selmer* 群 $S^{(m)}(E/K)$ は有限群である.

$E[m] \subset E(K)$ の場合に Selmer 群の有限性が示され, 従って weak Mordell-Weil の定理が示される．一般に $E[m] \not\subset E(K)$ の場合も

定理 1.59 *Selmer* 群 $S^{(m)}(E/K)$ は有限群である．従って, $E(K)/mE(K)$, $Ш(E/K)[m]$ はともに有限である.

Weak Mordell-Weil の定理が導かれた現時点でこの節の目標は達成されたのであるが, descent 列, Kummer 列についてもう少し詳しく眺めてみる．m-Kummer 列と m^r-Kummer 列のもとになった長完全列について, 図式

$$\begin{array}{ccccccccc}
E(K) & \xrightarrow{[m^r]} & E(K) & \xrightarrow{\delta} & H^1(\mathrm{G}_K, E[m^r]) & \longrightarrow & H^1(\mathrm{G}_K, E(\overline{K})) & \xrightarrow{[m^r]} & H^1(\mathrm{G}_K, E(\overline{K})) \\
\downarrow{\scriptstyle [m^{r-1}]} & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \alpha_r} & & \downarrow{\scriptstyle [m^{r-1}]} & & \downarrow{\scriptstyle id} \\
E(K) & \xrightarrow{[m]} & E(K) & \xrightarrow{\delta} & H^1(\mathrm{G}_K, E[m]) & \longrightarrow & H^1(\mathrm{G}_K, E(\overline{K})) & \xrightarrow{[m]} & H^1(\mathrm{G}_K, E(\overline{K}))
\end{array}$$

を考える．真ん中の準同型 $\alpha_r : H^1(\mathrm{G}_K, E[m^r]) \to H^1(\mathrm{G}_K, E[m])$ 以外のものは自然に定義されるものをとるとき, この図式が可換になるよう α_r を定義することができる．m-Kummer 列と m^r-Kummer 列からなる可換図式が得られる．K の各有限素点 v に対しても, 局所体上の Kummer 列の可換図式と $\alpha_{r,v} : H^1(\mathrm{G}_{K_v}, E[m^r]) \to H^1(\mathrm{G}_{K_v}, E[m])$ を同様の手順で得ることができる．α_r と $\alpha_{r,v}$ は局所化写像と可換になるから, Selmer 群の準同型

$$\alpha_r : S^{(m^r)}(E/K) \longrightarrow S^{(m)}(E/K)$$

が引き起こされる．また上の長完全列の可換図式から, Shafarevich-Tate 群の m-part と m^r-part の間の準同型

$$[m^{r-1}] : Ш(E/K)[m^r] \longrightarrow Ш(E/K)[m]$$

も得られる．m-descent 列と m^r-descent 列の可換図式

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/m^rE(K) & \xrightarrow{\delta} & S^{(m^r)}(E/K) & \longrightarrow & Ш(E/K)[m^r] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \alpha_r} & & \downarrow{\scriptstyle [m^{r-1}]} & & \\
0 & \longrightarrow & E(K)/mE(K) & \xrightarrow{\delta} & S^{(m)}(E/K) & \longrightarrow & Ш(E/K)[m] & \longrightarrow & 0
\end{array}$$

を得る.

命題 1.60 (1) $E(K)/mE(K) \simeq \mathrm{Im}\,\delta \subset \cdots \subset \mathrm{Im}\,\alpha_r \subset \cdots \subset \mathrm{Im}\,\alpha_2 \subset \mathrm{Im}\,\alpha_1 = S^{(m)}(E/K)$

(2) $\mathrm{Im}\,\delta = \mathrm{Im}\,\alpha_r$ であるための必要十分条件は, $[m^{r-1}]Ш(E/K)[m^r] = O$ である.

m-decent 列からくる埋め込み $E(K)/mE(K) \simeq \delta(E(K)/mE(K)) \subset S^{(m)}(E/K)$ を通して, $S^{(m)}(E/K)$ の中で $E(K)/mE(K)$ を調べる手続きのことを, **first m-descent** という．m^2-descent

列による埋め込み $E(K)/mE(K) \subset \alpha_2(S^{(m^2)}(E/K)) \subset S^{(m)}(E/K)$ を通して, $S^{(m)}(E/K)$, $S^{(m^2)}(E/K)$ の中で $E(K)/mE(K)$ を解析することを **second m-descent** という. 以下同様に r^{th} **m-descent** という $E(K)/mE(K)$ を解析する手続を考えることができる. もちろん, descent は $E(K)/mE(K)$ を使って Selmer 群や Galois cohomology $H^1(\mathrm{G}_K, E[m])$, 代数体の整数論的性質を導くのに使うこともできるわけで, descent 列を使った数論の解析手続のことを **descent procedure** (あるいは単に **descent**) という.

上の命題の (2) によると, $Ш(E/K)[m^r]$ が m^{r-1}-倍写像で消えていれば $E(K)/mE(K)$ は本質的に $\alpha_r(S^{(m^r)}(E/K))$ に一致する. つまりこのとき r^{th} m-descent により $E(K)/mE(K)$ を直接知ることができる. Shafarevich-Tate 群の "m-巾 part" を知りたくなる.

Shafarevich-Tate 群の m-part は定義をしたが, "Shafarevich-Tate 群" そのものはまだ定義していない. これからその定義をする. $m \,|\, m'$ について, m-倍写像で消える $H^1(\mathrm{G}_K, E(\overline{K})$ の元は m'-倍写像で消えるから, 自然な埋め込み $\iota : H^1(\mathrm{G}_K, E(\overline{K}))[m] \to H^1(\mathrm{G}_K, E(\overline{K}))[m']$ は, Shafarevich-Tate 群の m-part の m'-part への埋め込み

$$\iota : Ш(E/K)[m] \hookrightarrow Ш(E/K)[m']$$

を引き起こす. Shafarevich-Tate 群の m-part の帰納系の帰納極限として **Shafarevich-Tate 群**

$$Ш(E/K) = \varinjlim Ш(E/K)[m]$$

を定義することができる.

Hasse の原理 "局所的な情報をつなぎ合わせて, 大域的な情報を得たい" というものがある. Shafarevich-Tate 群 (の m-part) の定義をみると, "局所的には区別の出来ない大域的なもの" を集めたものになっている. Shafarevich-Tate 群が消えていれば, Hasse の原理が成り立ち, めでたしめでたしなのだが, Shafarevich-Tate 群は相当難解な対象なのでそう安直に話は進まない. Shafarevich-Tate 群 (m-part ではない) が有限かどうかもまだわかっていない. p-巾部分 ($Ш(E/K)[p^\infty] = \varinjlim Ш(E/K)[p^r]$) でさえ, 有限位数かどうかまだわかっていない.

予想 1.61 *Shafarevich-Tate* 群 $Ш(E/K)$ は有限群である.

定理 1.62 (Rubin) *Shafarevich-Tate* 群が有限群になる, *CM*-型楕円曲線の無限族が存在する.

定理 1.63 (Cassels, Tate, 大域双対定理) K を代数体 K, E/K を楕円曲線とする. このとき, 双線形な *pairing*

$$Ш(E/K) \times Ш(E/K) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

が存在する. さらに *Shafarevich-Tate* 群が有限群なら, この *pairing* は非退化である.

この pairing の具体的な構成などはここではやりません. "Modular Forms and Fermat's Last Theorem" (Cornell-Silverman-Stevens ed. Springer) の Silverman の記事などを参考にして下さい. この定理の系として得られることですが,

定理 1.64 *Shafarevich-Tate* 群の位数が有限なら, その位数は平方数である.

定理 1.65 *Shafarevich-Tate* 群のすべての p-巾部分の位数が有限なら, *Shafarevich-Tate* 群の位数は平方数である.

m-倍準同型から m-descent 列を与えたが, 一般に同種写像 $\lambda : E \to E'$ に対して全く同様の手続きで λ-Selmer 群 $S^{(\lambda)}(E/K)$, Shafarevich-Tate 群の λ-part $Ш(E/K)[\lambda]$ を定義し, λ-descent 列を与えることができますが, ここでは略します. Silverman (Springer GTM 106, 151), Husemöller (Springer GTM 111) の教科書的な楕円曲線の入門書などを参考にして下さい.

§1.10　Height 関数, Mordell-Weil の定理, Elliptic regulator

K を代数体, M_K を K の素点 (有限も無限も) の全体とする. K 上 Weierstrass 標準形で定義された楕円曲線 E に対して,

$$\begin{array}{rcl} h\colon E(K) & \longrightarrow & [0,\,\infty) \\ P & \longmapsto & \displaystyle\sum_{v\in M_K} \log \max(|x(P)|_v,\,1) \end{array}$$

を E/K の **height 関数**という.

命題 1.66 (a) $h([m]\,P) = m^2\,h(P) + O(1)$.
(b) $h(P+Q) + h(P-Q) = 2\,h(P) + 2\,h(Q) + O(1)$.
(c) 任意の $X > 0$ に対して *height* 関数の値が X 以下の $E(K)$ の点は有限個.

この命題の (a) より E の任意の K-有理点 P に対して $\lim\limits_{e\to\infty} 4^{-e}\,h([2^e]\,P)$ は収束する.

$$\begin{array}{rcl} \widehat{h}\colon E(K) & \longrightarrow & [0,\,\infty) \\ P & \longmapsto & \displaystyle\lim_{e\to\infty} 4^{-e}\,h([2^e]\,P) \end{array}$$

E/K の **canonical** (**Néron-Tate**) **height** という.

定理 1.67 (Néron-Tate) K を有限次代数体, E/K を楕円曲線, $\widehat{h}$ を *canonical height* とする.
(1) *canonical height* は $E(K)$ 上の半正定値 *2* 次形式である. すなわち,
(1-a) $\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\,\widehat{h}(P) + 2\,\widehat{h}(Q)$
(1-b) $\widehat{h}([m]P) = m^2\,\widehat{h}(P)$
(1-c) 次のものは双線形な *pairing* である. *(***Néron-Tate pairing** という.*)*

$$\begin{array}{rcl} \langle\,,\,\rangle_E\colon E(K)\times E(K) & \longrightarrow & \mathbb{R} \\ (P,\,Q) & \longmapsto & \widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q) \end{array}$$

(2) $\widehat{h}(P) = 0 \iff P \in E(K)_{\mathrm{tors}}$.
(3) $\widehat{h}(P) = h(P) + O(1)$.

ここまで準備ができると, Mordell-Weil の定理の証明を述べることができる. 前節で見た weak Mordell-Weil の定理より $E(K)/mE(K)$ は有限アーベル群だから, その代表系として $\{P_1,\cdots,P_n\}$ $(\subset E(K))$ をとる. $H = \max \widehat{h}(P_i)$, $M = \{P\in E(K)\,|\,\widehat{h}(P)\le H\}$ とおく. $\widehat{h}(P) = h(P) + O(1)$ だから, M は有限集合である.

$\langle M\rangle$ を M の元で張られた $E(K)$ の部分群とする. $E(K)\neq\langle M\rangle$ を仮定する. $Q\in E(K) - \langle M\rangle$ を canonical height が最小のものとする (このような Q のとれることは明らかである). $\{P_1,\cdots\}$ は $E(K)/mE(K)$ の代表系だったから, $Q = P_i + m\,R$ なる P_i, $R\in E(K)$ がとれる. $\widehat{h}(Q)$ の最小性と, 上で述べた $\widehat{h}$ の性質より,

$$\widehat{h}(Q) \le \widehat{h}(R) = \frac{1}{m^2}\,\widehat{h}([m]R) = \frac{1}{m^2}\,\widehat{h}(Q-P_i) \le \frac{2}{m^2}\,(\widehat{h}(Q) + \widehat{h}(P_i)) \le \frac{2}{m^2}\,(\widehat{h}(Q) + H)$$

従って, 今 $m > 1$ ととっているので,

$$\widehat{h}(Q) \le \frac{2}{m^2-2}\,H \le H$$

これは $Q\in M$ を意味し $Q\in E(K) - \langle M\rangle$ に矛盾する. (証明終り)

さて, Mordell-Weil の定理が証明されたので, $E(K)$ の階数の有限性がわかったことになる. P_1, $\cdots$, P_r を $E(K)/E(K)_{\mathrm{tors}}$ の代表系とする.

$$R(E/K) = \det(\langle P_i, P_j \rangle_E)_{i,j}$$

the elliptic regulator という. $r = 0$ のときには $R(E/K) = 1$ とおく.

命題 1.68 *$R(E/K)$ は $E(K)/E(K)_{\mathrm{tors}}$ の代表系の取り方に依らず, $R(E/K) > 0$.*

§1.11 導手, L-関数, Standard Conjectures

K を代数体, $\mathcal{O}_K$ を整数環, E/K を楕円曲線とする. K の各有限素点 v に対して, E の局所体 K_v 上の minimal Weierstrass model の判別式を Δ_v とおく. $\mathcal{O}_K$ のイデアル $\Delta_{E/K} = \prod_v \mathfrak{p}_v^{v(\Delta_v)}$ を E/K **の判別式**という. §1.1 で定義した Weierstrass model の判別式 Δ と異なることに注意. 明示的に区別するため, §1.1 で定義した判別式 Δ を "model の判別式", ここで定義した判別式 $\Delta_{E/K}$ を "楕円曲線としての判別式" と呼ぶことにする. §1.6 の最後の命題で述べたように j-不変量の値が代数的整数なら, その楕円曲線はどの有限素点上でも potentially good reduction をもつから, 定義体を有限次元の範囲で適当に拡大すればすべての有限素点上で good reduction をもつようにできる. このような, どの素点の上でも good reduction をもつ楕円曲線を **everywhere good reduction** をもつという. このとき楕円曲線としての判別式は (1) である.

整数環 $\mathcal{O}_K$-係数の Weierstrass model で定義された楕円曲線 E/K について, model の判別式 Δ が楕円曲線としての判別式 $\Delta_{E/K}$ を生成する ($\Delta_{E/K} = \Delta\mathcal{O}_K$) とき, その model を **global minimal Weierstrass model** という. 一般に楕円曲線が global minimal Weierstrass model をもつとは限らない.

命題 1.69 *有理数体上定義されたどの楕円曲線も global minimal Weierstrass model を持つ.*

次に楕円曲線の重要な不変量である "**導手** (**conductor**)" $N_{E/K}$ を定義する.

$$N_{E/K} = \prod_v \mathfrak{p}_v^{f_v(E/K)}$$

ただし,

$$f_v(E/K) = \begin{cases} 0 & E \text{ は } v \text{ で good reduction をもつ} \\ 1 & E \text{ は } v \text{ で multiplicative reduction をもつ} \\ 2+\delta_v & E \text{ は } v \text{ で additive reduction をもつ} \end{cases}$$

で, δ_v は ℓ-進表現の v での分岐の様子などから決まる非負の整数. 正確に定義するのは面倒なので省略する. Silverman GTM 106 などを参照のこと. 特に $\mathfrak{p}_v \nmid 6$ なら $\delta_v = 0$ で, $K = \mathbb{Q}$ なら $\delta_2 \leq 6$, $\delta_3 \leq 3$.

そして L-関数. E が v で good reduction をもつとき, $a_v = 1 - \sharp E(k_v) + q_v$ ($q_v = N\mathfrak{p}_v$) とおく.

$$L_v(T) = \begin{cases} 1 - a_v T + q_v T^2 & E \text{ は } v \text{ で good reduction をもつ} \\ 1 - T & E \text{ は } v \text{ で split multiplicative reduction をもつ} \\ 1 + T & E \text{ は } v \text{ で non-split multiplicative reduction をもつ} \\ 1 & E \text{ は } v \text{ で additive reduction をもつ} \end{cases}$$

とおく. **局所** L**-関数**という. 次で定義される Dirichilet 級数を, 楕円曲線 E/K の **Hasse-Weil** L**-関数**という.

$$L(E/K, s) = \prod_v L_v(q_v^{-s})^{-1}$$

命題 1.70 上の *Euler* 積は $\Re s > 3/2$ で広義一様に絶対収束する.

定理 1.71 *Hasse-Weil L*-関数は同種不変量である. すなわち, 代数体 K 上の楕円曲線 E, E' が K 上同種であることと, 測度 *0* の例外集合を除いた素点 v について $a_v(E) = a_v(E')$ であることとは同値である.

L-関数について幾つかの予想, 定理を, ... 何と言うか, まぁ知ってたらええのんちゃうやろか, ぐらいのノリで予想や定理を漫然と並べています. この節の以下の部分は付録と言うかおまけ程度に眺めるにとどめて下さい. この部分について真面目に研究, 勉強をするつもりなら, Silverman の本 (Splinger GTM 106) で取っ掛かりを作って, Cornell, Silverman, Stevens ed. "Modular Forms and Fermet's Last Theorem" などを読むとか, 近くの専門家にお聞き下さい.

予想 1.72 (Hasse-Weil) *Hasse-Weil L*-関数は, 全 s-平面に一価整関数に解析接続され, 関数等式

$$N_{E/K}^{s/2}(2\,\pi)^{-s}\Gamma(s)\,L(E/K,\,s) = w_{E/K}\,N_{E/K}^{1-s/2}(2\,\pi)^{s-2}\Gamma(2-s)\,L(E/K,\,2-s)$$

をもつ. ここで $w_{E/K}$ は関数等式の符号と呼ばれ ± 1 に値をとる.

定理 1.73 (Eichler-Shimura) $E/\mathbb{Q}$ を楕円曲線とする. $\mathbb{Q}$ 上の非定数有理射 $X_0(N) \to E$ が存在するとき, *level N*, *weight 2* の正規尖点形式 f で, その L-関数 $L_f(s)$ が E の *Hasse-Weil L*-関数 $L(E/\mathbb{Q},\,s)$ に一致するものが存在する. さらにこのことから, この楕円曲線に関して *Hasse-Weil* 予想が成り立つ.

予想 1.74 (Shimura-Taniyama, Modularity Conjecture) E を $\mathbb{Q}$ 上定義された, 導手 N の楕円曲線とする. L-関数 $L(E/\mathbb{Q},\,s)$ を *Mellin* 変換したものを $f(\tau)$ と書くとき, 次が成り立つ.
(1) $f(\tau)$ は *level N*, *weight 2* の *Hecke* 固有形式である. さらに, $(W\,f)(\tau) = f(-1/N\,\tau)$ とおくとき, $W\,f = w_{E/K}\,f$ *($w_{E/K}$ は関数等式の符号).*
(2) $\mathbb{Q}$ 上の有理射 $X_0(N) \to E$ が存在し, この射による不変微分 ω の引き戻しは *1-form* $f(\tau)\,d\tau$ の定数倍である.

定理 1.75 (Wiles, Diamond) $27 \nmid N$ ならば, *Shimura-Taniyama* 予想は正しい.

予想 1.76 (Birch and Swinnerton-Dyer) E を $\mathbb{Q}$ 上定義された, 導手 N の楕円曲線とする.
(1) *Hasse-Weil L*-関数 $L(E/\mathbb{Q},\,s)$ は $s = 1$ で $\operatorname{rank} E(\mathbb{Q})$ 位の *zero* をもつ.
(2) $R(E/\mathbb{Q})$ を *elliptic regulator*, $\Omega_\infty = \int_{E(\mathbb{R})} |\omega|$, $\Omega_p = \sharp E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, $r = \operatorname{rank} E(\mathbb{Q})$ とおく.

$$\lim_{s\to 1}(s-1)^{-r}\,L(E/\mathbb{Q},\,s) = \frac{\sharp Ш(E/\mathbb{Q})\,2^r\,R(E/\mathbb{Q})}{(\sharp E(\mathbb{Q})_{\mathrm{tors}})^2}\prod_{p\le\infty}\Omega_p$$

Birch と Swinnerton-Dyer は, 一般の代数体上でも同様な予想を述べている.

予想 1.77 (Birch and Swinnerton-Dyer) 有限次代数体 K 上定義された楕円曲線 E/K に対して, $L(E/K,\,s)$ は $s = 1$ で $\operatorname{rank} E(K)$ 位の *zero* をもつ.

これよりも弱い予想ではあるが, J. Coates は Shafarevich-Tate 群の構造と絡めた予想を提示している.

予想 1.78 (Coates)

$$\operatorname{ord}_{s=1}L(E/K,\,s) \ge \operatorname{rank} E(K)$$

等号の成立は *Shafarevich-Tate* 群が有限のときに限る.

“弱い” と言っても §1.9 の後の方で述べた Shafarevich-Tate 群の位数は有限である予想のもとでなら, 上の 2 つの予想は同等である. Birch and Swinnerton-Dyer の予想を裏付ける多くの結果がありますが, 申し訳ありませんが, ここでは割愛させて頂きます.

§2 等分点, Universal Boundness Conjecture

有限次代数体 K 上定義された楕円曲線 E の Mordell-Weil 群 $E(K)$ が有限生成アーベル群であること (Mordell-Weil の定理, §1.9, §1.10) に触れましたが, 以下ここでは特に等分点のなす部分群 $E(K)_{\mathrm{tors}}$ に関する話をします.

いつの頃からか, 多くの人々に信じられていた予想がありました.

予想 2.1 (Universal Boundness Conjecture) *K を代数体とする. K のみに依存する定数 C_K が存在して任意の楕円曲線 E/K に対して, $\sharp E(K)_{\mathrm{tors}} \leq C_K$.*

この予想について, p-巾部分は Ju. I. Manin による次の定理があります.

定理 2.2 (Manin (Izv. Akad. Nauk SSSR Ser. Mat. 33 (1969), 459-465)) *K を代数体, p を素数とする. K, p のみに依存する定数 $C_{K,p}$ が存在して, K 上定義された任意の楕円曲線 E/K に対して, $\sharp E(K)[p^\infty] \leq C_{K,p}$.*

有理数体上の場合に, “possible or impossible torsion” に関して具体的に多くの例が計算されていきました. “Possible torsion” は具体的に作って見せれば済むのですが, “impossible torsion” はどうやっても作れないことを示さねばなりません. Billing-Mahler (11-等分点, J. London Math. Soc. 15, (1940). 32–43), Ogg (17-等分点, Invent. Math. 12 (1971), 105–111), Mazur-Tate (13-等分点, Invent. Math. 22 (1973/74), 41–49) らによって, “impossible torsion” ($\mathbb{Q}$-有理等分点の位数として現われない整数) を決める技術が確立されていきました (cf. Kubert (Proc. London Math. Soc. (3) 33 (1976), no. 2, 193–237)). 簡単に雰囲気を言いますと, 楕円曲線の N-等分点の moduli が modular 曲線 $X_1(N)$ であることが認識され, その代数曲線の有理点の有無を調べれば有理 N-等分点をもつ楕円曲線の有無がわかる. 有理数体上の有理等分点については更に, modular 曲線 $X_1(N)$ が有理曲線であるか否かという, 代数幾何的な性質を調べるだけでわかる, というものです. 有理数体上定義された楕円曲線の有理等分点について, A. P. Ogg (Bull. Amer. Math. Soc. 81 (1975), 14–27) が予想し, B. Mazur により

定理 2.3 (Mazur (Springer LNM 601 (1977), 107–148)) *有理数体上定義された楕円曲線の有理等分点の全体は, 次の 15 個の群のいずれかに同型である.*

$$\begin{array}{ll} \mathbb{Z}/n\mathbb{Z} & n = 1, 2, \cdots, 10, 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\,m\mathbb{Z} & m = 1, 2, 3, 4 \end{array}$$

有理数体上の Universal Boundness Conjecture が解決した. この定理がどの様に示されたかなど詳細が柳井氏の解説にあります. 次は, 2 次体, 3 次体など一般の代数体上での Universal Boundness Conjecture を調べることになります. 有理数体上の場合のときと同じように, 適当な代数体を選んでその体ごとに調べることもされていましたが, Kamienny は Universal Boundness Conjecture を代数体ごとに述べた先の形ではなく, 体の拡大次数ごとに考える次の形に再定式化しました. 一般の代数体の場合にも moduli $X_1(N)$ の幾何学的な性質を調べることで予想が解決されるという筋書ができました.

予想 2.4 (Universal Boundness Conjecture) $d > 0$ を正の整数とする.

$$S(d) = \left\{ p : \text{素数} \;\middle|\; \begin{array}{l} \text{高々 } d \text{ 次の代数体 } K \text{ と } K \text{ 上の楕円曲線 } E \text{ で,} \\ K\text{-有理 } p\text{-等分点をもつものが存在する.} \end{array} \right\}$$

とおくとき, $S(d)$ は有限集合になる.

Kamienny のこの予想はもともとの予想に比べて, 代数体を固定せず次数を固定した点では強いことを言っているが, 等分点の位数の有界性でなく等分点の位数の素因子の有界性を言っている点では弱い予想になっている. 高々 d 次の代数体 K 上の楕円曲線の K-有理等分点のなす群として現われる有限アーベル群の同型類を $\Phi(d)$ とおくとき, Manin の定理と Demjanenko の方法により (詳細は Kamienny-Mazur (Astérisque No. 228 (1995), 3, 81–100, 1992 年の Columbia 大学での数論セミナーでの講演の記録) を参考にして下さい.)

命題 2.5 $S(d)$ が有限集合なら, $\Phi(d)$ もまた有限集合である.

従って Kamienny の予想を示せば十分であることがわかります. $d = 1$ の場合は Mazur の定理で, $S(1) = \{2, 3, 5, 7\}$, $\Phi(1)$ は Mazur の定理の 15 個のアーベル群.

定義体が 2 次体の場合, Kamienny (Bull. Amer. Math. Soc. (N.S.) 23 (1990), no. 2, 371–373, Invent. Math. 109 (1992), no. 2, 221–229) は $S(2)$ が有限集合であること

定理 2.6 (Kamienny)

$$S(2) = \{2, 3, 5, 7, 11, 13\}$$

を示し, Universal Boundness Conjecture ($d = 2$) を証明しました. また $\Phi(2)$ は Kenku-Momose (Nagoya Math. J. 109 (1988), 125-149) に具体的に決定されています. ちょっと考えると $\Phi(2)$ の決定が $S(2)$ の決定より先であるのは変に思えます. Kenku-Momose は, 17 以上の素数が $S(2)$ に含まれないという仮定 (予想) のもとで, $\Phi(2)$ の取りうるすべてを与えたものです. Kamienny によってその仮定が満たされることが示されたので, Kenku-Momose により $\Phi(2)$ が決定されたことになったわけです. 有理数体上の Mazur の定理の場合もそうでしたが, "$S(d)$ の上限が○○以下なら $\Phi(d)$ は△△に限る" が先に示され, その後 $S(d)$ の上限がその仮定を満たす程度に評価され, $\Phi(d)$ が得られるという手順になっています. 連名にすべきかどうか迷いますが, 2 次体上の楕円曲線の有理等分点についてすべてをまとめたと言うことで了承して頂けると思います.

定理 2.7 (Kamienny-Kenku-Momose) *2* 次体 K 上定義された楕円曲線の有理等分点は, 次の有限アーベル群のいずれかに同型である.

$$\begin{array}{ll} \mathbb{Z}/n\mathbb{Z} & n = 1, 2, \cdots, 14, 16, 18 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\,m\mathbb{Z} & m = 1, 2, \cdots, 6 \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\,m\mathbb{Z} & m = 1, 2 \quad (K = \mathbb{Q}(\sqrt{-3})) \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & (K = \mathbb{Q}(\sqrt{-1})) \end{array}$$

Kamienny-Mazur (Astérisque No. 228 (1995), 3, 81–100) は, $d \leq 8$ の場合に $S(d)$ が有限集合であることを証明し, 一般の d に対して $S(d)$ が素数全体の中で測度 0 であることを示しました. Abramovich (Astérisque No. 228 (1995), 3, 5–17) は Kamienny-Mazur の証明をより精密に行うことで $d \leq 12$ の場合に $S(d)$ が有限集合であることを証明しました. こうして一般の d に対して Universal Boundness Conjecture を証明するための技術ができてきたのですが, 最終的には,

定理 2.8 (Merel (Invent. Math. 124 (1996), no. 1-3, 437-449)) *2 以上の整数 d に対して, $S(d)$ に現われる素数 p は $d^{3\cdot d^2}$ を越えない. 特に $S(d)$ は有限集合で, Universal Boundness Conjecture が成立する.*

予想は解決されました. あとは, $\Phi(d)$ $(d \geq 3)$ を具体的に決めていくことになるのでしょうが, これらについては現在ほとんど何もわかっていません. 先にも書きましたが, $S(d)$ の適当な上限を仮定すれば $\Phi(d)$ を決めることができるはず $\cdots$ なのですが, 話はそんなに単純なものではありません. 上限があるのでそこまで modular 曲線を調べていけばいいわけですが, そのこと自身易しい問題ではありません. Merel の定理による $S(d)$ の評価にも問題があります. 大きすぎるのです. 例えば $d = 2$ のとき Merel の定理での $S(d)$ の評価は,

$$2^{3\cdot 2^2} = 2^{12} = 4096$$

です. $\Phi(2)$ を得るための $S(2)$ の上限は 17 でした. $d = 3$ だと

$$3^{3\cdot 3^2} = 3^{27} = 7.6 \times 10^{12}$$

有限であることに変りはありませんが, これだけ大きいと, どうしましょう. この評価をなんとか実用に耐える程度に良くしたいのが今後のひとつの目標といえます. Silverberg (Contemp. Math. 133 (1992), 175-193) は CM 型のアーベル多様体の有理等分点について重要な結果を得ているが, それを特に 1 次元アーベル多様体 (楕円曲線のこと) の場合に限定するなら,

定理 2.9 (Silverberg) *$d > 0$ とする. E を虚 2 次体 k を CM 体にもつ, d 次代数体 K 上定義された CM 型楕円曲線とする. このとき E の K-有理等分点の位数 N は, $\varphi(N) \leq \delta\,\mu\,d$ を満たす. ただし, μ は $\mathrm{End}(E)$ に含まれる 1 の巾根の個数, $\delta = 1/[K \cap k : \mathbb{Q}]$ ($k \subset K$ なら $\delta = 1/2$, そうでなければ $\delta = 1$).*

予想というか, 妄想, いや言葉が悪い. ひとつの大きな問いですが, "$S(d)$ に属する素数を d の多項式 (できれば d の 1 次式) で上から評価できないであろうか." ここでは, 1 次元に限定して Silverberg の定理を引用しましたが, 一般次元の本来の形 (一般の有限次代数体上定義された一般次元の CM 型アーベル多様体の有理等分点の位数の上からの評価) を見るとこの様な評価があってもいいような気がしますし, どこで見たのか忘れてしまい文献を引用できず申しわけありませんが, この様な予想を出してはる方々も沢山いてはります. ついでにもう一言, その Silverberg の定理も, 数値だけでみるなら, $\mathbb{Q}$ 上定義された CM 型 2 次元アーベル多様体の有理等分点の位数は 185640 以下であるとしか評価出来ない. 私の主観ですが, 大きすぎます. その平方根を取ったぐらいでもやや大きいと思いますが, 多分その程度ではないかと思います.

§3 楕円曲線の Mordell-Weil rank

楕円曲線の Mordell-Weil 群の rank については, 大雑把に 2 種類の予想がある. と言っても "予想" と言えたものか良くわかりませんが.

予想 3.1 *いくらでも rank の大きな楕円曲線 $/\mathbb{Q}$ が存在するだろう.*

予想 3.2 *定義体, あるいは, 定義体の次数を固定したとき, そこで定義される楕円曲線の rank は有界だろう.*

見てわかる通り相反する予想で, なんやねん, なんのこっちゃ, て具合いですが, どちらもそれなりに信じるべき根拠があり, ... まぁ何ともかんとも. rank が有界でないと言う話の中にはさらに,

予想 3.3 同種類に制限しても *rank* は有界でないだろう.

予想 3.4 同型類に制限しても *rank* は有界でないだろう.

予想 3.5 与えられた有理等分点をもつ楕円曲線の中にいくらでも大きな *rank* を持つものがあるだろう.

予想 3.6 与えられた楕円曲線について, その *(2* 次*) twist* の中にいくらでも大きな *rank* を持つものがあるだろう.

予想 3.7 有理等分点の構造なり, j-不変量なり, *rank* の大きさを決めてしまうことのない条件を適当に仮定しても, $\mathbb{Q}$ 上で同型でない楕円曲線 *(*$\overline{\mathbb{Q}}$ 上同型でも構わない*)* が無数に含まれるなら, その中にいくらでも *rank* の大きなものがあるだろう.

などと言うのんまであるにはあります.

ここ 10 年ほどの間の "rank の世界記録" の変遷について眺めることにします. 簡単な記号を準備しておきます.

$$BRank(K, (\text{条件})) = \sup\{\operatorname{rank} E(K) \mid E \text{ は (条件) を満たす体 } K \text{ 上の楕円曲線 }\}$$
$$BRank_\infty(K, (\text{条件})) = \limsup\{\operatorname{rank} E(K) \mid E \text{ は (条件) を満たす体 } K \text{ 上の楕円曲線 }\}$$

いい加減な記号です. "(条件)" というのは, 例えば $j = 0$ などのように j がいくらであるとか, 群 G が書いてあるときには $E(\mathbb{Q})_{\mathrm{tors}} \simeq G$ とか, 楕円曲線に関する条件が書かれます. 何も書かれていないときは, そういった制約条件を仮定しないときです. $BRank(\mathbb{Q}(T))$ と $BRank_\infty(\mathbb{Q})$ はよく似ていますが, パラメータ付きで構成されているか, 単に無数に存在することがわかっているものかの違いがあります.

- $\mathbb{Q}(T)$ 上定義されたもの

  J.-F. Mestre (1991) $BRank(\mathbb{Q}(T)) \geq 11$
  C. R. Acad. Sci. Paris Sér. I Math. 313 (1991), no. 3, 139–142

  J.-F. Mestre (1991) $BRank(\mathbb{Q}(T)) \geq 12$
  C. R. Acad. Sci. Paris Sér. I Math. 313 (1991), no. 4, 171–174

  K. Nagao (1994) $BRank(\mathbb{Q}(T)) \geq 13$
  Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), no. 5, 152–153

  J. Scholten (1998) $BRank(\mathbb{Q}(T)) \geq 14$
  preprint, 1998

- $\mathbb{Q}$ 上定義されたもの

  J.-F. Mestre (1992) $BRank(\mathbb{Q}) \geq 15$
  C. R. Acad. Sci. Paris Sér. I Math. 314 (1992), no. 6, 453–455

  K. Nagao (1992) $BRank(\mathbb{Q}) \geq 17$
  Proc. Japan Acad. Ser. A Math. Sci. 68 (1992), no. 9, 287–289

S. Fermigier (1992) $BRank(\mathbb{Q}) \geq 19$
C. R. Acad. Sci. Paris Sér. I Math. 315 (1992), no. 6, 719–722

K. Nagao (1993) $BRank(\mathbb{Q}) \geq 20$
Proc. Japan Acad. Ser. A Math. Sci. 69 (1993), no. 8, 291–293

K. Nagao-T. Kouya (1994) $BRank(\mathbb{Q}) \geq 21$
Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), no. 4, 104–105

S. Fermigier (1997) $BRank(\mathbb{Q}) \geq 22$
Acta Arith. 82 (1997), no. 4, 359–363

Martin-McMillen (1998 ?) $BRank(\mathbb{Q}) \geq 23$
Silverberg によれば 1998, Silverman によれば 1997
(立命館大学 (に移られた) の加川さんに教えて頂きました.)

S. Kihara (1997) $BRank_{\infty}(\mathbb{Q}) \geq 14$
Proc. Japan Acad. Ser. A Math. Sci. 73 (1997), no. 2, 32

- $j = 0$ または 1728, j-不変量を指定する.

S. Kihara (1987) $BRank_{\infty}(\mathbb{Q}, j = 0, 20$ 個以上の整数点をもつ$) \geq 5$
Proc. Japan Acad. Ser. A Math. Sci. 63 (1987), no. 3, 76–78

J.-F. Mestre (1992) $BRank(k(T), j = 0) \geq 6$ (k は標数が 2 でない任意の体)
C. R. Acad. Sci. Paris Sér. I Math. 314 (1992), no. 12, 919–922

J.-F. Mestre (1992) $BRank(k(T), j = 1728) \geq 4$ (k は標数が 2 でない任意の体)
C. R. Acad. Sci. Paris Sér. I Math. 314 (1992), no. 12, 919–922

K. Nagao (1994) $BRank(\mathbb{Q}(T), j = 1728) \geq 4$
Kobe J. Math. 11 (1994), no. 2, 205–210

J.-F. Mestre (1995) $BRank_{\infty}(\mathbb{Q}, j = 0) \geq 7$
C. R. Acad. Sci. Paris Sér. I Math. 321 (1995), no. 9, 1235–1236

S. Kihara (1996) $BRank_{\infty}(\mathbb{Q}, j = 0) \geq 7$
Proc. Japan Acad. Ser. A Math. Sci. 72 (1996), no. 10, 228–229

E. Liverance (1998) $BRank(\mathbb{Q}(T), j = j_0) \geq 2$, $BRank(\mathbb{Q}(\sqrt{-1}, T), j = j_0) \geq 3$
Manuscripta Math. 99 (1999), 1-11

- 有理等分点を指定する

P. L. Montgomery (1987) $BRank(\mathbb{Q}, G) \geq 1$ (G は Mazur の定理に出てくる 15 個のアーベル群)
Math. Comp. 48 (1987), no. 177, 243–264

A. O. L. Atkin-F. Morain (1993) $BRank(\mathbb{Q}, G) \geq 1$ (G は Mazur の定理に出てくる 15 個のアーベル群)
Math. Comp. 60 (1993), no. 201,399–405

S. Fermigier (1996) $BRank(\mathbb{Q}(T), \mathbb{Z}/2\mathbb{Z}) \geq 8$
C. R. Acad. Sci. Paris Sér. I Math. 322 (1996), no. 10, 949–957

S. Fermigier (1996) $BRank(\mathbb{Q}(t_1, t_2, t_3, t_4, t_5), \mathbb{Z}/2\mathbb{Z}) \geq 8$
Springer LN in Comput. Sci., 1122 (1996), 115–120,

S. Fermigier (1996) $BRank(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \geq 14$ (rank が丁度 12, 13, 14 である $E/\mathbb{Q}$ を構成した.)
Springer LN in Comput. Sci., 1122 (1996), 115–120,

K. Nagao (1997) $BRank_\infty(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \geq 8$
Math. Comp. 66 (1997), no. 217, 411–415

S. Kihara (1997) $BRank_\infty(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \geq 9$
Proc. Japan Acad. Ser. A Math. Sci. 73 (1997), no. 9, 165

S. Kihara (1997) $BRank_\infty(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \geq 4$
Proc. Japan Acad. Ser. A Math. Sci. 73 (1997), no. 5, 77–78

S. Kihara (1997) $BRank_\infty(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \geq 5$
Proc. Japan Acad. Ser. A Math. Sci. 73 (1997), no. 8, 151

L. Kulesz (1997) $BRank_\infty(\mathbb{Q}, \mathbb{Z}/3\mathbb{Z}) \geq 6$, $BRank_\infty(\mathbb{Q}, \mathbb{Z}/4\mathbb{Z}) \geq 3$, $BRank_\infty(\mathbb{Q}, \mathbb{Z}/5\mathbb{Z}) \geq 2$, $BRank_\infty(\mathbb{Q}, \mathbb{Z}/6\mathbb{Z}) \geq 2$, $BRank_\infty(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \geq 4$, $BRank_\infty(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \geq 2$
preprint, 1997

A. Dujella (1998) $BRank(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \geq 7$
preprint, 1998

A. Dujella (1999) $BRank(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \geq 8$
Internet mailing list “Number Theory List”, 1999

$\mathbb{Q}$ 上の Mordell-Weil rank の高い楕円曲線を作る方法は, だいたい次のような手順になります. $\mathbb{Q}$-係数の関数体上の楕円曲線で generic に rank の高いものを作ります. それを $\mathbb{Q}$ に特殊化 (specialize) したものをたくさん作り, そのそれぞれについて Hasse-Weil L-関数を計算します. といっても, 高々有限個の素数について局所 zeta 関数を計算するだけしかできませんが... Birch and Swinnerton-Dyer の予想を手がかりに, L-関数の zero 点の order が大きくなりそうか大雑把に判定することで, 楕円曲線を篩にかけます. 例えば, rank が大きいということは有理点が多いということだから, reduction したときの有限体上の楕円曲線は有理点を多くもつでしょう... などと考え, この場合なら例えば $p < 1000$ について $\mathbb{F}_p$-有理点が最大か最大に近いものだけをとる. という “篩” を作るわけです. Mestre (Compositio Math. 58 (1986), no. 2, 209–232), Nagao (Kobe J. Math. 11 (1994), no. 2, 211–219, Math. Comp. 66 (1997), no. 217, 411–415) などを参考にしてください. この方法に従って rank の高いものを効率良く得るには,

(1) 判別が容易で有効な “篩” を見つける.

(2) 特殊化して rank の大きなものが出てきそうな関数体上の楕円曲線をみつける.

$E/\mathbb{Q}(T)$ を $\mathbb{Z}[T]$ に係数をもつ Weierstrass 方程式で定義された楕円曲線とする. $c_4 = c_4(T)$, $c_6 = c_6(T)$ は最初に定義した model から決まる量で, $\Delta = \Delta(T)$ を判別式, $j = j(T)$ を j-不変量とする. c_4, c_6, Δ は T に関する $\mathbb{Z}$-係数多項式.

$$N(T) = \prod_{\Delta(\alpha)=0} (T - \alpha) \prod_{c_4(\alpha)=c_6(\alpha)=0} (T - \alpha)$$

とおき, $E/\mathbb{Q}(T)$ の **conductor 多項式**という. T を $t \in \mathbb{Z}$ or $\mathbb{Q}$ に特殊化したときの楕円曲線を $E_t/\mathbb{Q}$ と書く. 対象として特殊化した楕円曲線の rank の平均を考える.

$$\frac{1}{2X} \sum_{|t| \leq X} \operatorname{rank} E_t(\mathbb{Q})$$

この上限は

定理 3.8 (Michel (Monatsh. Math. 120 (1995), no. 2, 127–136)) *Standard Conjectures* のもとで,

$$\frac{1}{2X} \sum_{|t| \leq X} \operatorname{rank} E_t(\mathbb{Q}) \leq (\deg \Delta(T) + \deg N(T) - \frac{3}{2})\,(1 + O(1)) \qquad as\ \ X \to \infty$$

定理 3.9 (Silverman (preprint, 1997)) *Standard Conjectures* のもとで,

$$\frac{1}{2X} \sum_{|t| \leq X} \operatorname{rank} E_t(\mathbb{Q}) \leq (\deg N(T) + \operatorname{rank} E(\mathbb{Q}(T)) - \frac{1}{2})\,(1 + O(1)) \qquad as\ \ X \to \infty$$

下限の方は, 一般に特殊化で rank は落ちないから,

$$\frac{1}{2X} \sum_{|t| \leq X} \operatorname{rank} E_t(\mathbb{Q}) \geq \operatorname{rank} E(\mathbb{Q}(T)) + O(1/X) \qquad \text{as}\ \ X \to \infty$$

がわかる. ただこれは, 実験的だが, とても小さいと思われている. Standard Conjectures のもとで $E_t/\mathbb{Q}$ の L-関数 $L(E_t/\mathbb{Q}, s)$ の関数等式の符号は, ± 1 の間で同じような分布をすることが知られている. これは, E_t の中で rank が奇数のものと偶数のものが半々であることを言っているから

$$\frac{1}{2X} \sum_{|t| \leq X} \operatorname{rank} E_t(\mathbb{Q}) \geq \operatorname{rank} E(\mathbb{Q}(T)) + \frac{1}{2} + O(1/X) \qquad \text{as}\ \ X \to \infty$$

多くの人々によりこの下限の精度を良くする研究がなされている. Fermigier (Experiment. Math. 5 (1996), no. 2, 119–130) の実験データによると, geniric rank が $0 \sim 4$ の 93 個の $\mathbb{Q}(T)$ 上の楕円曲線について, 66918 個の特殊化した楕円曲線の rank を計算したところ,

$$\operatorname{rank} E_t(\mathbb{Q}) - \operatorname{rank} E(\mathbb{Q}(T)) = \begin{cases} 0 & 32\ \% \\ 1 & 48\ \% \\ 2 & 18\ \% \\ 3 & 2\ \% \end{cases}$$

Brumer-McGuinness (Bull. Amer. Math. Soc. (N.S.) 23 (1990), no.2, 375–382) にも同じようなデータがある. $\mathbb{Z}$-係数の Weierstrass model の楕円曲線で, $|\Delta|$ が 10^8 以下の素数で $|a_6| \leq 2^{31} - 1$ なるものをすべて求め (311243 個ある), rank を計算したところ,

rank	0	1	2	3	4	5
個数	93337	143192	61517	11861	804	5
平均	30.04 %	46.08 %	19.80 %	3.82 %	0.26 %	-

$E/\mathbb{Q}$ を導手 N の modular 楕円曲線とし, $F = \sum a_n\, q^n$ を対応する $\Gamma_0(N)$ の newform とする. w を L-関数 $L(s, F) = L(E/\mathbb{Q}, s)$ の関数等式における符合とする. D を 2 次体の判別式とし, ξ_D を対応する 2 次の指標とする. $L_(s, F_D) = \sum \xi_D(n)\, a_n\, n^{-s}$ は, E の $\mathbb{Q}(\sqrt{D})$ に関する

2 次 twist E_D の L-関数になっている．また D が N と素なら, $L(s,\, F_D)$ の関数等式の符合は $w_D = w\,\xi_D(-N)$ である．$r \geq 1$ に対して,

$$M_F^r(X) = \sharp\{D : |D| < X,\, \mathrm{ord}_{s=1} L(s,\, F_D) = r\}$$

とおく.

予想 3.10 (Goldfeld (Springer LNM 751 (1979), 108–118))

$$M_F^0(X) \sim M_F^1(X) \sim X/2 \qquad as\ \ X \to \infty$$

Kolyvagin, Gross-Zagier の結果より, $L(1,\, F_D) \neq 0$ なら $\mathrm{rank}\, E_D(\mathbb{Q}) = 0$, $w_D = -1$ で $L'(1,\, F_D) \neq 0$ なら $\mathrm{rank}\, E_D(\mathbb{Q}) = 1$ だから, この予想は rank $= 0$ と rank $= 1$ の楕円曲線が約半分ずつあって, rank ≥ 2 のものは測度的には 0 であると言っている．弱い形になっているが,

定理 3.11 (Iwaniec-Sarnak (preprint, 1997)) 一般 *Riemann* 予想のもとで

$$M_F^r(X) \gg X \qquad as\ \ X \to \infty \qquad (r = 0,\, 1)$$

Riemann 予想を仮定しないなら

定理 3.12 (Ono-Skinner (to appear in Invent. Math.))

$$M_F^0(X) \gg X/\log(X)$$

定理 3.13 (Perelli-Pomykala (Acta Arith. 80 (1997), no. 2, 149–163))

$$M_F^1(X) \gg_\varepsilon X^{1-\varepsilon}$$

他にも有理等分点とか reduction の型などに条件をつけたものとか, Cremona's Tables ("Algorithms for elliptic curves", Cambridge Univ. Press, 2nd ed. 1997) などから選んだ幾つかの modular 楕円曲線に対して, Riemann 予想を仮定せずに Iwaniec-Sarnak の評価式が得られている．この辺の話については, Vatsal (Math. Ann. 311 (1998), 791–794) の前半にまとめてあります.

楕円曲面の rank に関する Nagao 予想について話します．K を有限次代数体, $\mathfrak{p}$ を素イデアル, $k_\mathfrak{p}$ を剰余体, $q_\mathfrak{p}$ をその位数とする．C/K を K 上の非特異射影曲線, E/K を non-split elliptic surface で, $E \to C$ は C 上 regular, proper で K 上定義されているとする．K-有理 section $C \to E$ のなす有限生成アーベル群の階数を, $\mathrm{rank}\, E(C/K)$ とおく．$x \in C(k_\mathfrak{p})$ で E を特殊化したものを E_x とおく．$a_\mathfrak{p}(E_x)$ を E_x が非特異のとき $1 - \sharp E_x(k_\mathfrak{p}) + q_\mathfrak{p}$, split-multiplicative のとき $+1$, non-split-multiplicative のとき -1, additive のとき 0 とおく．その平均

$$A_\mathfrak{p}(E) = \frac{1}{q_\mathfrak{p}} \sum_{x \in C(k_\mathfrak{p})} a_\mathfrak{p}(E_x)$$

とおくとき,

予想 3.14 (Nagao (Manuscripta Math. 92 (1997), no. 1, 13–32)) $K = \mathbb{Q}$, $C = \mathbb{P}^1$ のとき,

$$\lim_{X \to \infty} \frac{1}{X} \sum_{p \leq X} -A_p(E)\, \log p = \mathrm{rank}\, E(\mathbb{P}^1/\mathbb{Q})$$

これを Rosen-Silverman (preprint, 1997) が

予想 3.15 (Nagao-Rosen-Silverman)

$$\mathrm{Res}_{s=1} \sum_{\mathfrak{p}} -A_{\mathfrak{p}} \frac{\log q_{\mathfrak{p}}}{q_{\mathfrak{p}}^{s}} = \mathrm{rank}\, E(C/K)$$

と一般化し,

定理 3.16 (Rosen-Silverman) *Standard Conjectures* のもとで, *Nagao-Silverman* の予想が成り立つ.

$E_{a,b} : y^2 = x^3 + a\,x + b$ とします. 最後に何やら意味のよくわかんない不思議な評価式を 2 つ挙げます.

定理 3.17 (Fouvry (Progr. Math., 108, (1993)))

$$\sum_{0<|t|\leq T} \sqrt{3}^{\mathrm{rank}\, E_{0,t}(\mathbb{Q})} = O(T)$$

定理 3.18 (Heath-Brown (Invent. Math. 111 (1993), 171–195))

$$\sum_{0<|t|\leq T} \sqrt{2}^{\mathrm{rank}\, E_{-t^2,0}(\mathbb{Q})} = O(T)$$

§4 参考文献など

第 1 章では, 楕円曲線論の基礎と思われるところの概略をまとめてみました. 予定では, 題にもあるように同種写像の話題も盛り込むつもりでしたが, そこまで手が廻りませんでした. 楕円曲線の定義からはじめて大雑把に一通り, 楕円曲線論を読み進めていけるよう書いたつもりです. 詳しい説明, 証明, 例などはすべて割愛しましたので, すぐには理解しづらいところもあるかも知れません. もっとも, 不明確な文章や, 誤字脱字などのタイプミス, 論理的に間違えているところなどあるかもしれません. 以下の文献を参照して下さい. 楕円曲線論の重要な部分を占める, 虚数乗法論には一切ふれていません. 以下の文献をご覧下さい.

毎日のように新しい結果, 新しい話題, 新しい解釈が出されています. 2 章, 3 章は, いつまでたっても筆の止まらない, いつまでたっても書き直しの終わらない, どつぼにはまったような感があります. これ以降の加筆訂正などは, 申し訳ありませんが, InterNet 上の私のページの

`http://www2.math.sci.osaka-u.ac.jp/~ogawa/Ellip_Cur/`

をご覧下さい.

J. W. S. Cassels, "Lectures on Elliptic Curves", Student Texts 24, London Math. Soc., 1991
大変易しく読めます. 後半 Galois cohomology が出てきたあたりから, 書いてることがわけわからんようになるので, そこからは他の本を読んだほうが良いでしょう.

J. H. Silverman and J. Tate, "Rational Points on Elliptic Curves", Springer UTM, 1992
これも易しく書いてあります. 演習問題も見ながら読んでいくと, 有理数体上の楕円曲線の幾何になれることが出来るでしょう.

J. H. Silverman, "The Arithmetic of Elliptic Curves", Springer GTM 106, 1985
"楕円曲線論の教科書" と言ってもいいでしょう. 最初の代数幾何のような準備のところは, いい加減に書いてあります.

D. Husemöller, “Elliptic Curves”, Springer GTM 111, 1986
Silverman の本と比較するなら, 流れは丁寧に書かれていますが, 行間の意を汲む必要のあるところがやや多く感じます. Silverman のより, 新しいことが書かれていますが, 読んだ後, 何となくいつも定義体が $\mathbb{Q}$ のものを扱ってたような気になります.

岩澤 健吉, “代数函数論 増補版”, 岩波書店, 1973
なにはともあれ, 緒言を読んでみましょう. 示唆に富んでとても面白いことでしょう.

J. W. S. Cassels, “Diophantine Equations with Special Refernce to Elliptic Curves”, J. London Math. Soc. 41 (1966), 193–291
Silverman の本の出る前はこれがひとつにまとめられた入門書だったそうです.

A. W. Knapp, “Elliptic Curves”, Princeton Univ. Press
標準的な楕円曲線の入門と, 楕円関数論, 保型形式と 3 方面から書かれており, それぞれの角度から楕円曲線論に入っていけます. Eichler-Shimura 理論の解説がこの本の主目的です. もともと表現論の人で, Langlands ... に向かっています. 最後の Notes にいろいろ書いてあります.

J. H. Silverman, “Advanced Topics in the Arithmetic of Elliptic Curves”, Springer GTM 151, 1994
何と言いますか, Silverman 自身の Springer GTM 106 の続編ということなのですが, 前のんほど読みやすくはありません. 前のに書けなかった面白いけどちょっと難しい話題を集めてあります. 楕円関数, 虚数乗法論の部分は他の本を勧めます. 楕円曲面, Néron model は他の代数幾何の専門書では難しく感じた方も, Silverman の前の本で楕円曲線を勉強した方ならわかりやすく感じるのではないでしょうか.

J.-P. Serre, “Abelian ℓ-adic Representations and Elliptic Curves”, Benjamin, 1968
ℓ-進表現の入門書です. 4 章に楕円曲線上の話が丁寧に書いてあります.

J. E. Cremona, “Argorithms for Modular Elliptic Curves, 2nd ed.”, Cambridge Univ. Press, 1997
めくってわかる通り楕円曲線の表 (Cremona’s Table) です. 導手の順に並べてあります. “[導手 (数字)][同種類 (alphabet)][同型類 (番号)]” で modular 楕円曲線をこの表から引用されます. 例えば, “11A1” は $y^2 + y = x^3 - x^2 - 10\,x - 20$ で modular 曲線 $\mathfrak{H}/\Gamma_0(11)$ のことです. Antwarp IV (Springer LNM 476) の表 (導手 200 以下) を導手 1000 以下に広げたものです. InterNet 上で 5300 以下の表が公開されています. (1998 年 9 月)
`ftp://euclid.ex.ac.uk/pub/cremona`
日本からなら
`ftp://tnt-ftp.math.sci.osaka-u.ac.jp/ftp/Cremona`

H. Cohen, “A Course in Computational Algebraic Number Theory”, Springer GTM 138, 1995
整数論の定理には実際の計算にそのまま使えるものが多いのですが, アルゴリズムとともに大変使いやすくまとめてあります.

S. Lang, “Elliptic Curves Diophantine Analysis”, Springer, 1978
Mordell の “Diophantine Equations” (Acad. press, 1969) を批判して, そんでもって書かれ

たものですが, どちらも良い本です. 後から書かれた Lang の本の方が現代的というのはまぁ当たり前でしょう. Baker 理論への入門に.

H. McKean and V. Moll, “Elliptic Curves”, Cambridge Univ. Press, 1997
楕円関数から始めていく場合の入門書と言っていいかと思います. 楕円積分から現在の楕円曲線論への端緒を見いだしていった道筋をたどって書かれています.

A. Borel, S. Chowla, C. S. Herz, K. Iwasawa and J. P. Serre, “Seminar on Complex Multiplication”, Springer LNM 21, 1966
虚数乗法論の教科書と言ってもいいてしょう. 虚 2 次体の類数 1 問題の解けていないときに書かれたものですが, かえっていろいろ示唆にとんだところがあります. 短いので 1 週間ぐらいで虚数乗法論が勉強できます.

志村 五郎, 谷山 豊, “近代的整数論”, 共立出版, 1957
高次元も含めて虚数乗法論が日本語で読めますが, 真面目に勉強するなら次に挙げている 2 冊の方がいいと思います. 最初の章の歴史を読んでみましょう. その章の最後まで読んだとき, きっと虚数乗法論について思いを新たにすることでしょう.

G. Shimura and Y. Taniyama, “Complex Multiplication of Abelian Varieties and its Applications to Number Theory”, Math. Soc. Japan, 1961

G. Shimura, “Abelian Varieties with Complex Multiplication and Modular Functions”, Princeton, 1997
前半は上の本と同じでです. 後半, 内容を新しくし, また現代の視点から書き改められています.

G. Shimura, “Arithmetic Theory of Automorphic Functions”, Princeton Univ. Press, 1971
楕円曲線は 4 章にあります. 楕円曲線の虚数乗法論, 高次元アーベル多様体の虚数乗法論を勉強できるでしょう.

S. Lang, “Elliptic Functions, 2nd ed.”, Springer GTM 112, 1987
あ, 手元にない. どんなんやったっけ? 確か, Part I が楕円関数の話で, Part II が虚数乗法論. Part III ってあったかなかったか忘れてしまいました.

G. Cornell, J. H. Silverman and G. Stevens ed, “Modular Forms and Fermet’s Last Theorem”, Springer, 1997
2 章に Silverman による楕円曲線論の survey があります.

J. W. S. Cassels and E. V. Flynn, “Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2”, London Math. Soc. Lecture Note Ser. 230, Cambridge Univ. Press, 1996
種数 2 の代数曲線に関してまとめられた初めての本です.