第5章

楕円曲線の岩澤理論について

栗原 将人 (東京都立大学 理学研究科)

サマースクールでは上記の表題のもとに講演したのだが、後半部分で話した内容は熟し切っていないので別の機会に譲ることにし、前半で話した内容を中心として、基本的なことから書いていきたい。

§1. Spirit of Iwasawa

楕円曲線の有理点全体のなす群は、楕円曲線の整数論で最も重要で基本的な対象だが、L-関数にその情報が含まれているという有名な Birch Swinnerton-Dyer 予想と呼ばれる予想がある。E を $\mathbf{Q}$ 上に定義された楕円曲線、$E(\mathbf{Q})$ を Mordell Weil 群（$\mathbf{Q}$-有理点全体）とすると、$E(\mathbf{Q})$ は Mordell の定理により有限生成 abel 群である（cf. Silverman [6] Chapter 8)。一方、$L(E,s)$ を L-関数とする（cf. [6] Appendix §16）と、$L(E,s)$ は $\mathbf{C}$ 全体で正則であると予想（Hasse Weil 予想）される（現在では Wiles 及びそれに続く仕事により、ほとんどの楕円曲線でこれは確かめられている)。$L(E,s)$ が $\mathbf{C}$ 上の正則関数であるとして、Birch と Swinnerton-Dyer は、

$$\mathrm{order}_{s=1} L(E,s) = \mathrm{rank} E(\mathbf{Q}) \tag{1}$$

と予想し、また $L(E,s)$ の Taylor 展開の最初の係数を数論的な量で表す予想を提出した (cf. Silverman [6] page 362)。

整数論的に非常に重要な対象と、zeta 関数の値との間の不思議な関係は、整数論の重要なテーマの一つだが、この予想はその典型的な例である。

この予想に対し、最初の大きな前進は 1977 年の Coates Wiles [1] による次の結果である。すなわち、E が虚数乗法を持つとき、(1) の左辺が 0 であれば、右辺も 0 であるというのである（つまり、$L(E,1) \neq 0$ ならば $\#E(\mathbf{Q}) < \infty$)。

この論文 [1] の序文には、何故かこの論文が "spirit of Iwasawa" で書かれたのだ、ということが強調されている。(この論文の証明を普通に読んでも、いわゆる $\mathbf{Z}_p$-拡大に関する岩澤理論の雰囲気はないのだが。) さらに、将来のさらなる発展、たとえば Tate Shafarevich 群の有限性を証明するのに、岩澤理論的考え方が最重要な役割を果たすだろう、とある。このことが実現されるためには、この論文からさらに約十年の歳月が必要であったのだが (Rubin [4])、岩澤理論というものが楕円曲線の理論にどのような役に立つのか、という質問をされたとして、この論文の序文ほどはっきりとした答はないだろう。何しろ、Birch Swinnerton-Dyer 予想という大きな予想の最初の大きな一歩を踏み出した論文にこう書いてあるのだから。

論文 [1] に大きな影響を与えた“spirit of Iwasawa” とは、具体的にはまず local units の群を円単数群で割ったものと、Riemann zeta 関数の値との関係である。この関係について詳しく述べる前に、岩澤理論が (1) のような予想にどのように役に立つのか簡単な様子を書いておきたい。

Coates Wiles, Rubin 等の証明は、普通にはつながりにくい L-関数という解析関数と $E(\mathbf{Q})$ を、p 進世界を経由することでつなぐのである。仮に Iwasawa Main Conjecture を認めると、全体像は非常にすっきりとして、次のように書ける。すなわち、(E は p で good reduction を持つとして)

$$
\begin{aligned}
L(E,1)=0 &\iff p\text{ 進 }L\text{ 関数が }s=1\text{ に零点を持つ}\\
&\overset{(*)}{\iff} \text{Selmer 群の位数が無限}\\
&\Longleftarrow E(\mathbf{Q})\text{ の位数が無限}
\end{aligned}
$$

ここで、最初の同値関係は p-進 L 関数の定義から得られるもの(普通の L-関数の値を補間する p-進関数として p-進 L 関数は定義される)、(*) は Iwasawa Main Conjecture からの結論(§2 §3 で解説する)、最後の関係は Selmer 群の定義(§2 §3 で述べる)から得られるものである。岩澤理論は、上のように p-進解析的対象と p-進代数的対象を結ぶ理論であり、このような形で (1) のような問題に使えるのである。次の節では古典的岩澤理論を復習し、最後に上の (*) についてもう少し詳しく説明する。

§2. 岩澤理論(classical case)

χ を Dirichlet 指標、K を $\mathrm{Ker}\chi$ に対応する代数体(つまり $\mathrm{Gal}(K/\mathbf{Q})\simeq \mathrm{Image}\,\chi$)とする。素数 p を固定し、μ_{p^n} を 1 の p^n 乗根全体がなす群、K_∞/K を円分 $\mathbf{Z}_p$-拡大($K(\mu_{p^\infty})$ の中に含まれる唯一の $\mathbf{Z}_p$-拡大)、K_n を次数 p^n の中間体とする。A_{K_n} を K_n のイデアル類群の p-成分(p-Sylow 群)とし、

$$X_{K_\infty}=\varprojlim A_{k_n}$$

(Norm による逆極限)とおく。$\Delta=\mathrm{Gal}(K/\mathbf{Q})$ とおき、X_{K_∞} を $\mathbf{Z}_p[\Delta]$-加群とみる。χ を第一種指標である($\mathbf{Q}_\infty$ を $\mathbf{Q}$ の円分 $\mathbf{Z}_p$-拡大とするとき、$\mathbf{Q}_\infty\cap K=\mathbf{Q}$)と仮定し、$X_{K_\infty}$ の χ-成分を

$$X_{K_\infty}^{\chi}:=X_{K_\infty}\otimes_{\mathbf{Z}_p[\Delta]}O_\chi \qquad O_\chi=\mathbf{Z}_p[\mathrm{Image}\,\chi]$$

で定義する。ここで Δ は χ を通じて $O_\chi=\mathbf{Z}_p[\mathrm{Image}\,\chi]$ に作用するものとする。$\Gamma=\mathrm{Gal}(K_\infty/K)$ として $\Lambda=O_\chi[[\Gamma]]:=\varprojlim O_\chi[\Gamma/\Gamma^{p^n}]$ とおき、$X_{K_\infty}^{\chi}$ を Λ-加群とみる。このとき、$X_{K_\infty}^{\chi}$ は有限生成 torsion Λ-加群になる。

一般に有限生成 torsion Λ-加群 M に対し、M の特性イデアルとよばれる Λ のイデアル $\mathrm{char}(M)$ が次のようにして定まる。Λ-準同型写像 $\varphi: M\longrightarrow \Lambda/(f_1^{n_1})\oplus\ldots\oplus\Lambda/(f_r^{n_r})$ でその核、余核が有限となるものが存在する。このとき、$\mathrm{char}(M)=(f_1^{n_1}\cdot\ldots\cdot f_r^{n_r})$ と定義するのである(φ のとり方によらない)。$\mathrm{char}(M)$ は M の構造に関し、最初の基本的な量である。

Γ の任意の指標 $\psi:\Gamma\longrightarrow\overline{\mathbf{Q}}_p^{\times}$ に対して、それを線形性と連続性により $\Lambda=O_\chi[[\Gamma]]$ に延長した写像も $\psi:\Lambda\longrightarrow\overline{\mathbf{Q}}_p$ と書くことにする。Γ の生成元 γ を一つとって、γ と

$1+T$ を対応させることにより、Λ を $O_\chi[[T]]$ と同一視することができる。このとき、上の定義は、$f(T)\in O_\chi[[T]]$ に対し、$\psi(f(T))=f(\psi(\gamma)-1)$ を意味している。

κ を Γ の cyclotomic character（任意の 1 の p 巾根 ζ に対して、$\kappa(\sigma)=\zeta^{\kappa(\sigma)}$ をみたす指標）、ω を Teichmüller character とする。このとき、有名な Iwasawa Main Conjecture とは odd な χ（$\chi(-1)=-1$）に対する $X^\chi_{K_\infty}$ の次の性質である。(なおここに、$X^\chi_{K_\infty}$ はイデアル類群の $-$ 部分（マイナス部分）に関連していることに注意しておく。)

定理（Iwasawa Main Conjecture、Mazur Wiles の定理）
χ を $\chi\neq\omega$ をみたす odd な指標（$\chi(-1)=-1$）とするとき、

(2) $$\mathrm{char}(X^\chi_{K_\infty})=(\frac{1}{2}G_{\chi^{-1}\omega}).$$

ここに、$G_{\chi^{-1}\omega}\in\Lambda$ は、正の整数 $r>0$ に対して

$$\kappa^{1-r}(G_{\chi^{-1}\omega})=(1-\chi^{-1}\omega^{1-r}(p)p^{r-1})L(1-r,\chi^{-1}\omega^{1-r})$$

（$L(s,\chi^{-1}\omega^{1-r})$ は Dirichlet L-関数）をみたす元である。

$s\in\mathbf{Z}_p$ に対して、$\kappa^s:\Gamma\longrightarrow\mathbf{Z}_p^\times$ が自然に定義されることに注意する。$G_{\chi^{-1}\omega}$ を使ってできる $\mathbf{Z}_p$ から $\overline{\mathbf{Q}_p}$ への関数 $s\mapsto\kappa^s(G_{\chi^{-1}\omega})$ は Kubota-Leopoldt の p-進 L 関数とよばれる p-進解析関数で、普通 $L_p(s,\chi^{-1}\omega)$ と書かれる。つまり、$G_{\chi^{-1}\omega}$ は p-進 L 関数のもとなる元であり、ここでは $G_{\chi^{-1}\omega}$ のことを p-進 L 関数とよぶことにする。

定理の左辺はイデアル類群という数論的なもの、右辺は p-進解析的なもので、この定理はこのような異なる両者を結びつけるものであることに注意しよう。

Iwasawa Main Conjecture には別の定式化もある。特にイデアル類群の $+$ 部分（プラス部分）を使ったものは大事なので、それについて述べていく。

1 を像が $\{1\}$ であるような指標（trivial 指標）として、今度は χ を 1 でない even な指標（$\chi(-1)=1$）とする。

まず、v を p の上の K_n の素点として、v での完備化 $K_{n,v}$ の principal units 全体を $U^1_{K_{n,v}}$、$U_{K_n}=\Pi_{v|p}U^1_{K_{n,v}}$、$\mathcal{U}_{K_\infty}=\varprojlim U_{K_n}$ とおき、また U_{K_n} の中で円単数全体の位相的閉包をとってできる群の逆極限を $\mathcal{C}_{K_\infty}$ と書く（cf. [7] Chap 8, 13)。$\mathcal{U}_{K_\infty}/\mathcal{C}_{K_\infty}$ の χ-成分の特性イデアル $\mathrm{char}((\mathcal{U}_{K_\infty}/\mathcal{C}_{K_\infty})^\chi)$ が p-進 L 関数で書けることが岩澤先生によって証明された。これが、[1] で "spirit of Iwasawa" として最初に取り上げられた関係である（と言ってよいと思う）。

一方、$\mathcal{X}$ を K_∞ の p の外で不分岐な pro-p abel 拡大のうち最大のものの Galois 群とすると、Kummer dual により X^χ と $\mathcal{X}^{\chi^{-1}\omega}$ が対応する。上から Iwasawa Main Conjecure は、1 でない even な指標 χ（$\chi(-1)=1$）に対して

(3) $$\mathrm{char}(\mathcal{X}^\chi)=\mathrm{char}((\mathcal{U}_{K_\infty}/\mathcal{C}_{K_\infty})^\chi)$$

と書き直すことができる。

また、U_{K_n} の中で K_n の単数群の位相的閉包の逆極限を $\mathcal{E}_{K_\infty}$ と書くと、類体論により完全系列

$$0 \longrightarrow (\mathcal{E}_{K_\infty}/\mathcal{C}_{K_\infty})^\chi \longrightarrow (\mathcal{U}_{K_\infty}/\mathcal{C}_{K_\infty})^\chi \longrightarrow \mathcal{X}_{K_\infty}^\chi \longrightarrow X_{K_\infty}^\chi \longrightarrow 0$$

が得られる。そこで Iwasawa Main Conjecture は次のようにも定式化される。

定理（Iwasawa Main Conjecture 第二の定式化）
χ が $\chi(-1)=1$、$\chi \neq 1$ をみたすとき、

$$\text{char}(X^\chi) = \text{char}((\mathcal{E}_{K_\infty}/\mathcal{C}_{K_\infty})^\chi) \tag{4}$$

この定理は最初の定式化と同値であり、従って最初に Mazur と Wiles により証明されたのだが、その後 Kolyvagin のあみだした Euler system の手法により、Rubin, Greither により直接証明された。

Remark. 最後に Coates Wiles による証明の方針の概略を、§1 で述べた（*）をもう少し詳しく解説する形で述べよう。E は虚二次体の整数環 O_K による虚数乗法を持つとし、p を good ordinary reduction を持つ素数とし、K での分解を $(p)=\wp\overline{\wp}$ と書く。K_∞ を E の $\wp$ 巾等分点をすべて付け加えて得られる体とし、$\mathcal{U}_{K_\infty}$ を上のような local units とすると、このときは円単数のかわりに楕円単数というよいものが存在する。楕円単数がなす部分群を $\mathcal{C}_{K_\infty}$ と書くと、$\wp$-進 L 関数 $L_\wp(E,s)$ というものがあって、岩澤先生の定理の類似が成り立ち、$\mathcal{U}_{K_\infty}/\mathcal{C}_{K_\infty}$ と関係する。さらに、$\mathcal{U}_{K_\infty}/\mathcal{C}_{K_\infty}$ は、この場合の Iwasawa Main Conjecture により、K_∞ の $\wp$ の外で不分岐、pro-p abel な最大の拡大の Galois 群 $\mathcal{X}$ と関係する（cf. 上の（3））。$\mathcal{X}$ は定義から Selmer 群 $\text{Sel}=\text{Sel}(E/K_\infty, E[\wp^\infty])$ と関係するので、結論として $L_\wp(E,s)$ は Sel と関係する。（なおこの Iwasawa Main Conjecture はイデアル類群と楕円単数の群との関係であり、円単数の役割を楕円単数が果たすことにより、（4）の Euler system を使った証明と同じ方法で証明できる。cf. [5]）

そこで、$\#E(\mathbf{Q})=\infty$ と仮定すると、$E(\mathbf{Q})\otimes K_\wp/O_{K_\wp}$ が Selmer 群の中に入っていることから（cf. §3）、$\#(\text{Sel})^\Gamma=\infty$ （ここに $\Gamma=\text{Gal}(K_\infty/K)$）が得られる。上に述べた Iwasawa Main Conjecture を認めれば、このことは $\#(\mathcal{U}_{K_\infty}/\mathcal{C}_{K_\infty})_\Gamma=\infty$ を導き、さらには $L_\wp(E,1)=0$、及び $L(E,1)=0$ を導くのである。（Coates Wiles のもともとの証明は、ひとつの素数を使うものではなく、たくさんの素数を使ってなされる（無限個の素数で割れる数は 0 ということを使う）。しかし、上のような考え方は、それこそ "spirit of Coates and Wiles" として論文の中からくみとることができる。）

§3. 楕円曲線の場合

ここでは楕円曲線の Iwasawa Main Conjecture について、なるべく簡単な言葉で述べていこう。E を $\mathbf{Q}$ 上に定義された modular な楕円曲線とし、素数 p を一つ固定する。代数体 F に対して、$E[p^\infty]$ を代数閉包 $\overline{F}$ 有理点 $E(\overline{F})$ の中の p 巾分点全体とし、Galois cohomology $H^1(F,E[p^\infty]) = H^1(\text{Gal}(\overline{F}/F), E[p^\infty])$ を考える。完全系列 $0 \longrightarrow E[p^n] \longrightarrow E(\overline{F}) \xrightarrow{p^n} E(\overline{F}) \longrightarrow 0$ から cohomology をとって得られる完全系列 $0 \longrightarrow$

$E(F)/p^nE(F) \longrightarrow H^1(F, E[p^n]) \longrightarrow H^1(F, E(\overline{F}))$ の順極限をとって、$0 \longrightarrow E(F) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow H^1(F, E[p^\infty]) \longrightarrow H^1(F, E(\overline{F}))$ が得られる。v を F の素点として、F の v での完備化 F_v でも上と同様に $E(F_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p$ を $H^1(F_v, E[p^\infty])$ の部分群と見ることにより、$H^1(F, E[p^\infty])$ の部分群 $\mathrm{Sel}(E/F)$ （$E[p^\infty]$ に関する Selmer 群）を

$$\mathrm{Sel}(E/F) = \mathrm{Ker}(H^1(F, E[p^\infty]) \longrightarrow \prod_{v:\text{all primes}} \frac{H^1(F_v, E[p^\infty])}{E(F_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p})$$

で定義する。ここに v は F のすべての素点を走る。定義から、完全系列

$$0 \longrightarrow E(F) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}(E/F) \longrightarrow Ш(E/F)[p^\infty] \longrightarrow 0$$

が得られる。ここに、$Ш(E/F)[p^\infty]$ は Tate Shafarevich 群
$Ш(E/F) = \mathrm{Ker}(H^1(F, E(\overline{F})) \longrightarrow \Pi_v H^1(F_v, E(\overline{F}_v)))$ の p 巾で消える元全体である。（一般に $E(F)$ を知ることは難しいが、局所体での条件で定義される $\mathrm{Sel}(E/F)$ を計算することはそれよりずっと易しい。しかし、局所的に方程式が解を持つことと本当に大域的な F での解を持つことには ずれがあるので、そのずれが Tate Shafarevich 群として現れる。これが上の完全系列である。Tate Shafarevich 群が有限であるという予想は、この局所と大域のずれがたとえあっても有限の範囲でおさまることを言っている。）このように、$\mathrm{Sel}(E/F)$ は Mordell Weil 群と Tate Shafarevich 群の両方の情報を含む重要な群である。

以下では E は modular な楕円曲線であるとする。また、まず E は p で good ordinary reduction を持つとする。χ を第一種 Dirichlet 指標とし、K, K_∞, Λ を §2 のように定義する。また、$\mathcal{C}(E/K_\infty) = \mathrm{Hom}(\mathrm{Sel}(E/K_\infty), \mathbf{Q}_p/\mathbf{Z}_p)$ を $\mathrm{Sel}(E/K_\infty)$ の Pontrjagin dual とする。このとき、

定理. （E が虚数乗法を持つとき Rubin、持たないとき Kato）。
$\mathcal{C}(E/K_\infty)^\chi$ は有限生成 torsion Λ-加群

一方、ψ を conductor が p 巾の指標とするとき、$L(E, \chi\psi, 1)$ の値（正確には $L(E, (\chi\psi)^{-1}, 1)/\Omega_E^\pm$、$\Omega_E^\pm$ は period ）を補間する p-進 L 関数 $G_{E,\chi}$ が存在する（Mazur Swinnerton-Dyer [2]）。今のような ordinary の状況では、classical case と同様に $G_{E,\chi} \in \Lambda$ であり（正確には $G_{E,\chi} \in \Lambda \otimes \mathbf{Q}$ がわかっているが、$p \neq 2$ であれば、$G_{E,\chi} \in \Lambda$ は示されている（Mazur, Stevens, Vatsal））、$\psi(G_{E,\chi})$ が L 関数の値等を使って書けるのである。このとき、次が Mazur によって予想された classical な Iwasawa Main Conjecture の類似である。

予想.（Iwasawa Main Conjecture）
E が p で good ordinary reduction を持つとき

$$\mathrm{char}(\mathcal{C}(E/K_\infty)^\chi) = (G_{E,\chi}) \tag{5}$$

この予想に関しては、E が虚数乗法を持つとき、Rubin により証明されており、また虚数乗法を持たないとき、Tate module に対応する Euler system を構成することにより、

加藤和也先生によって、左辺がほぼ右辺を割るということ（p の巾を除いて左辺が右辺を割る）が証明されている。

イデアル類群に関する Iwasawa Main Conjecture を証明するときには、類数公式により左辺が右辺を割ることを示せば、等号が出る。しかし、楕円曲線については類数公式とは Birch Swinnerton-Dyer 予想そのものだから、証明に使うことはできず、片方の divisibility と等号との間には開きがあるのである。

この予想が正しければ、$\#\mathrm{Sel}(E/K_\infty)^\Gamma=\infty$ と $1(G_{E,\chi})=0$ つまり $L(E,1)=0$ とが同値であることは直ちに従う。これが、§1 の最後に（*）として述べた関係に他ならない。

§2 の Iwasawa Main Conjecture には第二の定式化（4）があった。我々は楕円曲線の場合にこの類似を考えることにしよう。ここで、Selmer 群 $\mathrm{Sel}(E/F)$ の次のような部分群 $\mathrm{Sel}_0(E/F)$ を考える。

$$\mathrm{Sel}_0(E/F)=\mathrm{Ker}(\mathrm{Sel}(E/F)\longrightarrow\prod_{v|p}E(F_v)\otimes\mathbf{Q}_p/\mathbf{Z}_p) \tag{6}$$

ここに、$\mathrm{Sel}(E/F)$ は $H^1(F,E[p^\infty])$ の部分群とみて、また $E(F_v)\otimes\mathbf{Q}_p/\mathbf{Z}_p$ は $H^1(F_v,E[p^\infty])$ の部分群とみて、自然な写像による kernel を考えている。また v は p を割る素点をすべて走る。§2 の Iwasawa Main Conjecture の第一の定式化（2）では、イデアル類群の $-$ 部分を使い、第二の定式化（4）ではイデアル類群の $+$ 部分を使った。上の $\mathrm{Sel}_0(E/F)$ がイデアル類群の $+$ 部分の類似であると我々は考える。

χ, K, K_n, K_∞ は上の通りとして、$\mathrm{Sel}_0(E/K_\infty)$ の Potrjagin dual $\mathcal{C}_0(E/K_\infty)=\mathrm{Hom}(\mathrm{Sel}_0(E/K_\infty),\mathbf{Q}_p/\mathbf{Z}_p)$ を考える。また、E は p で good reduction を持つとし、S を bad reduction を持つ素数と p とでできる素数の有限集合、K_S/K を $\overline{K}$ の中で S の外で不分岐な最大の拡大、$T=T_p(E)$ を Tate module として $\mathbf{H}^1_{K_\infty}=\varprojlim H^1(K_S/K_n,T)$ とおく。$\mathbf{H}^1_{K_\infty}$ の中には、加藤和也先生によって構成された（"最良"の）zeta elements（L 関数の値と結びつく Euler system）があるが、それらでできる部分群を Z_{K_∞} と書く。（これが円単数群の類似である。）このとき、

予想.（Iwasawa Main Conjecture 第二の定式化）
E が p で good reduction を持つとき

$$\mathrm{char}(\mathcal{C}_0(E/K_\infty)^\chi)=\mathrm{char}((\mathbf{H}^1_{K_\infty}/Z_{K_\infty})^\chi) \tag{7}$$

この予想は p が good ordinary のとき、最初の定式化（5）と同値である。

この定式化がすぐれているのは、p が ordinary でなくてもかまわない点である。実際、p が supersingular であるとすると、$\mathcal{C}(E/K_\infty)^\chi$ はもはや torsion Λ-加群にはならないが、$\mathcal{C}_0(E/K_\infty)^\chi$ は torsion Λ-加群となる。そこで上のような特性イデアルが考えられるのである。

また、$\mathrm{Sel}_0(E/K)$ には $\mathrm{Sel}(E/K)$ では成立しない次のような Control Theorem が成立する。簡単のため、$p \neq 2$ であるかあるいは E の判別式が負であると仮定すると、

$$\begin{aligned} H^1(\Gamma, H^0(K_\infty, E[p^\infty])) &\longrightarrow \mathrm{Sel}_0(E/K) \longrightarrow \mathrm{Sel}_0(E/K_\infty)^\Gamma \\ &\longrightarrow [\frac{\bigoplus_{v \in S_\infty} H^0(K_{\infty,v}, E[p^\infty])}{H^0(K_\infty, E[p^\infty])}]_\Gamma \end{aligned}$$

は完全系列になる。ここに、S_∞ は S の上にある K_∞ の素点の集合である。($\mathrm{Sel}_0(E/K) \longrightarrow \mathrm{Sel}_0(E/K_\infty)^\Gamma$ の核、余核が E と K_∞ だけによる数で押さえられていることに注意しよう。)

p が good reduction でないときにも上の予想と同様の定式化ができるが、ここでは省略する。またこの群 $\mathrm{Sel}_0(E/F)$ の応用、及び実例の計算については、別の機会に改めて書きたいと思う。

参考文献

[1] Coates J. and Wiles A., On the conjecture of Birch and Swinnerton-Dyer, Invent math 39 (1977), 223-251.

[2] Mazur B. and Swinnerton-Dyer, P., Arithmetic of Weil curves, Invent math 25 (1974), 1-61.

[3] Rubin K., Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, Invent math 64 (1981), 455-470.

[4] Rubin K., Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, Invent math 89 (1987), 527-560.

[5] Rubin K., The " main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent math 103 (1991), 25-68.

[6] Silverman J.H., *The arithmetic of elliptic curves*, Graduate Texts in Math 106 (1986), Springer-Verlag

[7] Washington L.C., *Introduction to cyclotomic fields*, Graduate Texts in Math 83 (1980), Springer-Verlag