数理解析研究所講究録
925巻 1995年 1-9

Birch－Swinnerton－Dyer予想の紹介

中島匠一

東京大学大学院 数理科学研究科

0. イントロダクション

この記事（講演の内容と同じ）では楕円曲線に関する Birch - Swinnerton-Dyer 予想（以下、ＢＳＤ予想、と呼ぶ）がどんなものかについて入門的紹介をして行く。入門と言っても、何も知らない所から始めるのは無理なので、ある程度の知識は仮定せざるをえなかった。スペースの関係（と筆者の力量）から、証明は一切しないし、説明を省いた所も多い。また、記号の定義を少なくするため、できるかぎり簡単な場合に限定して、一般的な定理についていちいち触れる事も避けた。という訳で、これから楕円曲線を勉強して行こうとしている学部学生、大学院生のための道案内、ぐらいに思って頂ければちょうど良いと思う。本格的に勉強する方は何らかの文献を参照して頂きたい。そう思って考えてみると、日本語の本が見当たらないのは残念である。しかし、英語の教科書はいくつか出ている。ここではもっとも代表的（と言っていいと思う）な Silverman の本だけを挙げておく：

J. H. Silverman : "The arithmetic of elliptic curves", GTM106, Springer (1986) .

本ではないが、J.Tate の、上と同名の論文（ Invent. math. 23 (1974) pp.179–206 ）もぜひ見て頂きたい。

ここで以下で使われる記号のうち一般的なものをリストしておく。

$\mathbf{N} = \{1, 2, ...\}$ は自然数の集合で、$\mathbf{Z}$ は整数環を表す。$\mathbf{Q}, \mathbf{R}, \mathbf{C}$ は各々、有理数体、実数体、複素数体である。素数 ℓ に対して、$\mathbf{Z}_\ell$ を ℓ 進整数環、$\mathbf{Q}_\ell$ をその商体とする。また、$\mathbf{F}_q$ で q 元体（ q は素数べき）を表す。Kを体とする時、$\mathrm{char}(K)$ 、$\overline{K}$ は各々、K の標数と代数的閉包を示すとする。

集合 A に対して、$|A|$ でその濃度（元の個数）を表す。また、整数 $a, b (a \neq 0)$ について、$a|b$ は a が b を割り切る事を示し、$a \not| b$ は $a|b$ の否定を表すとする。

1. 楕円曲線

Kを体とする。K上の楕円曲線 E（ E が K 上定義されている事を表すために E/K と書いたりする）というものの正確な定義は教科書を参照して頂く事にして、ここでは楕円曲線の3つのとらえ方を挙げておくだけにする：

(1) 1次元のアーベル多様体
(2) 種数1の代数曲線で $K-$ 有理点 O が与えられているもの
(3) 射影平面 $\mathbf{P}^2$ 内の非特異3次曲線で $K-$ 有理点 O が与えられているもの

楕円曲線 E 上には Oを原点とするアーベル群の構造が入っている事が大変重要である。

(3) がもっとも具体的であるが、座標の変換を考える事でもっと具体的に、次の様な表示がある事が分かる（簡単のため、$\mathrm{char}(K) \neq 2,3$ とする）:

$$(*) \qquad E : Y^2Z = X^3 + AXZ^2 + BZ^3 \qquad (A, B \in K).$$

ここで、$(X : Y : Z)$ は $\mathbf{P}^2$ の座標を表し、$O = (0 : 1 : 0) \in \mathbf{P}^2$ が与えられた有理点である。

$$\Delta = -16(4A^3 + 27B^2)$$

と置くと、「非特異」という条件は $\Delta \neq 0$ で表される。

(*) において $Z = 0$ となる点は O だけなので、この点を除いて、$x = X/Z, y = Y/Z$ として

$$(**) \qquad E : y^2 = x^3 + Ax + B$$

と表示する事もおおい。以下、E はこの形とする。これを Weierstrass normal form と呼ぶ。（これより複雑になるが任意の標数で通用する generalized Weierstrass normal form がある。）E の群構造を具体的に書き下すことができるが、ここでは省略する。

この記事では余り出てこないのだが、E にとって重要な量を与えておく。

$$j_E = 1728\frac{(4A)^3}{\Delta}$$

は、E の j 不変量と呼ばれ、E の $\overline{K}$ 上の同型類を決定する。また、$\omega = \mathrm{d}x/2y$ は E の第一種微分（正則微分）の基底を与える。これは E の群演算による平行移動に関して不変なので、E の不変微分とも呼ばれる。

K の拡大体 L が与えられた時、E の $L-$ 有理点全体を $E(L)$ で表す。つまり、

$$\begin{aligned} E(L) &= \{(X : Y : Z) \in \mathbf{P}^2 \mid X, Y, Z \in L, (X : Y : Z) \text{ は } (*) \text{ を満たす}\} \\ &= \{(x, y) \in L^2 \mid (x, y) \text{ は } (**) \text{ を満たす}\} \cup \{O\} \end{aligned}$$

である。E の群構造により、$E(L)$ は O を単位元とするアーベル群になる（演算を加法で表す）。

自然数 n に対し、E の n 等分点全体からなる群を E_n で表す：

$$E_n = \{P \in E(\overline{K}) \mid nP = O\}.$$

E_n の構造について次の定理がある（$p = \mathrm{char}(K)$ とする）。

Theorem 1. $p \nmid n$ なら $E_n \cong (\mathbf{Z}/n\mathbf{Z}) \oplus (\mathbf{Z}/n\mathbf{Z})$.

ℓ を p と異なる素数とする。$n \in \mathbf{N}$ に対し、「ℓ 倍する」事によって準同型 $E_{\ell^{n+1}} \to E_{\ell^n}$ が定まる。この系の射影極限をとって

$$T_\ell(E) = \varprojlim_n E_{\ell^n}$$

という $\mathbf{Z}_\ell-$ 加群ができる。これを E の（ℓ に関する）Tate 加群という。$T_\ell(E)$ は $\mathbf{Z}_\ell-$ 加群としては $\mathbf{Z}_\ell \oplus \mathbf{Z}_\ell$ に同型である（Theorem 1 による）に過ぎないが、$T_\ell(E)$ には $\mathrm{Gal}(\overline{K}/K)$ の作用があり、これが大変重要である。（K が有限体の場合は次節で少し触れる。）$T_\ell(E)$ は E の ℓ 進エタルコホモロジーとしても解釈できる。

最後に、$K = \mathbf{C}$ の場合にちょっと触れておこう。この時には $E(\mathbf{C})$ は複素多様体となり、complex torus と同型である事が知られている。具体的には、$\mathbf{C}$ 内のラティス $L = \mathbf{Z} + \mathbf{Z}\tau\,(\tau \in \mathbf{C}, \mathrm{Im}(\tau) > 0)$ が定まり、$E(\mathbf{C}) \cong \mathbf{C}/L$ となる。$E(\mathbf{C})$ の群構造は $\mathbf{C}/L$ に自然に入っている群構造と一致する。この場合は Theorem 1 の成立も理解し易いであろう。

2. 有限体上の楕円曲線

p を素数、q を p のべきとして、$K = \mathbf{F}_q$ （q 元体）の場合を考えてみよう。（この記事では、$q = p$ の場合のみ必要。）$n \in \mathbf{N}$ に対し、$E(\mathbf{F}_{q^n})$ は有限集合なので、

$$N^{(n)} = |E(\mathbf{F}_{q^n})| \qquad (\in \mathbf{N})$$

と置く。変数 u を取り、次の、u に関する形式的べき級数を考える（exp() は指数関数）:

$$Z(E/\mathbf{F}_q, u) = \exp(\sum_{n=1}^{\infty} N^{(n)} \frac{u^n}{n}).$$

これを $E/\mathbf{F}_q$ の合同ゼータ関数という。合同ゼータ関数は有限体上の代数曲線（さらには代数多様体）に対して考えられるものであり、その発生、研究の歴史はとても面白いが、ここでは省略する。合同ゼータ関数はリーマンのゼータ関数の類似として考えられた、という事だけいっておこう。

$Z(E/\mathbf{F}_q, u)$ に関する研究成果をまとめると次の様になる：

Theorem 2.

(1) （有理性）

$$a = q + 1 - N^{(1)}$$

とおく時、

$$Z(E/\mathbf{F}_q, u) = \frac{1 - au + qu^2}{(1-u)(1-qu)}$$

と表される。

(2) （関数等式）

$$Z(E/\mathbf{F}_q, 1/qu) = Z(E/\mathbf{F}_q, u)$$

が成立する。

(3) （リーマン予想の類似）

不等式

$$|a| \leq 2\sqrt{q}$$

が成り立っている。

$1 - au + qu^2 = (1 - \alpha u)(1 - \beta u) \quad (\alpha, \beta \in \mathbf{C})$ とする時、(3) は、「α, β は互いに複素共役」と同値であり、「$|\alpha| = |\beta| = \sqrt{q}$」とも同値である。この意味で (3) はリーマン予想の類似と見なされる。(2) は (1) からすぐ分かる（楕円曲線の場合）が、これもリーマンゼータ関数の関数等式の類似になっている。

最後に、合同ゼータ関数 $Z(E/\mathbf{F}_q, u)$ と Tate 加群との関係を述べて置こう。$\varphi_q(x) = x^q$ で $\varphi_q \in \mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$ を定めれば、φ_q は $T_\ell(E)$（$\ell(\neq p)$ は素数）に作用する（φ_q を Frobenius 写像という）。この時、

$$1 - au + qu^2 = \det(1 - \varphi_q u : T_\ell(E) \to T_\ell(E))$$

が成立している。これは Theorem 2 の証明に当たって大事な性質である。

3. 有理数体上の楕円曲線のＬ関数

これからは $K = \mathbf{Q}$ の場合を考えよう。（これが主題である。）(*) において $A, B \in \mathbf{Q}$ の場合を考える事になるが、（X, Y, Z を何倍かすることで）$A, B \in \mathbf{Z}$ としておこう。この時、$\Delta \in \mathbf{Z}$ である。ＢＳＤ予想は $E(\mathbf{Q})$ と E のＬ関数との関係を考えるものなので、この節では $E/\mathbf{Q}$ のＬ関数を導入しよう。p を素数とする時、(*) を reduction mod p すれば $\mathbf{F}_p$ 上の３次曲線が得られる。それを（良い記号を思い付かないので）$E \pmod p$ と表そう。$p \nmid \Delta$ なら、$E \pmod p$ は非特異となり $\mathbf{F}_p$ 上の楕円曲線となる。（この様な時、E は p で good reduction を持つ、とか、p は（E にとって）good prime である、とかと言う。）p が good な時、$\tilde{E} = E \pmod p$ として、$a_p = p + 1 - |\tilde{E}(\mathbf{F}_p)|$ と置き、

$$L_p(u) = 1 - a_p u + pu^2$$

とする（合同ゼータ関数 $Z(\tilde{E}/\mathbf{F}_p, u)$ の分子）。ここで、$E/\mathbf{Q}$ のＬ関数（変数 $s \in \mathbf{C}$ についての関数）を次で定義する：

$$L(E/\mathbf{Q}, s) = \prod_p L_p(p^{-s})^{-1}.$$

右辺はすべての素数に関する積である。（この様なものをオイラー積という。）さて、$p|\Delta$ なる素数 p（有限個である）については $L_p(u)$ を定義してないが、これらについては「うまく定義できる」とだけ言っておこう。正確な定義にはいろいろ準備が必要なのである。

$L(E/\mathbf{Q}, s)$ を上式で「定義する」と言ったが、右辺は無限積であるから収束が問題である。これについては Theorem 2 を使って次の事が分かる：

Theorem 3. *$L(E/\mathbf{Q}, s)$ は $\mathrm{Re}(s) > 3/2$ で絶対収束する（$\mathrm{Re}(s)$ は s の実部）。*

これにより $L(E/\mathbf{Q}, s)$ は $\mathrm{Re}(s) > 3/2$ で正則関数を定める事になるが、更に次の事が予想されている：

（Ａ） **Hasse-Weil 予想.** *$L(E/\mathbf{Q}, s)$ は $\mathbf{C}$ 全体に正則に延長される。*

関数等式についても予想がある。$E/\mathbf{Q}$ に対して $E/\mathbf{Q}$ の導手（conductor）と呼ばれる自然数 $N = N_E$ が定まる。N は重要な意味を持つ数であるが、（難しいので）正確な定義は省略する。$p \nmid \Delta \Longrightarrow p \nmid N$ が成立する事を指摘するにとどめて置こう。この N を使って、

$$\xi(E/\mathbf{Q}, s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E/\mathbf{Q}, s)$$

と置く。（π は円周率、$\Gamma(s)$ はガンマ関数である。）

（Ａ）の成立を前提として、関数等式は次の様に予想されている。

（B） 関数等式の予想.

$$\xi(E/\mathbf{Q}, 2-s) = -\epsilon\,\xi(E/\mathbf{Q}, s)$$

ここで、$\epsilon = \pm 1$ である。（ $-\epsilon$ も ± 1 であるが、都合により $-$ を付けておいた（下を見よ）。）

次の［CM］または［MOD］を満たす Eについては予想（A）（B）の成立が分かっている：

［CM］ E が虚数乗法を持つ（ CM type である）。つまり、E の $\overline{\mathbf{Q}}$ 上の自己準同型環 $\mathrm{End}(E)$ がある虚2次体 F の order である。

［MOD］$E/\mathbf{Q}$ は modular 楕円曲線である。つまり、modular 曲線 $X_0(N)$ から E への全射がある（ N は導手）。

ここで、$X_0(N)$ は

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \,|\, c \equiv 0 \pmod{N} \right\}$$

に対応する modular 曲線である。

［CM］の場合は $L(E/\mathbf{Q}, s)$ は F に関する Hecke のL関数によって表せる事が分かり、それによって（A）（B）が示せる。［MOD］の場合には、ある

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n \qquad (q = \exp(2\pi\sqrt{-1}\,\tau), \tau \in \mathbf{C}, \mathrm{Im}(\tau) > 0)$$

という $\Gamma_0(N)$ に関する符号（指標） ϵ の normalized cusp form で Hecke 作用素の同時固有関数になっているもの（説明は省略）があって、

$$L(E/\mathbf{Q}, s) = L(f, s) \quad (:= \sum_{n=1}^{\infty} a_n n^{-s})$$

が成り立つ事が分かっている。modular form の理論から $L(f, s)$ については解析接続、関数等式について良く分かっているので、（A）（B）が示せる事になる。

実は「［CM］$\Longrightarrow$［MOD］」が成立するので、結局、「 modular 楕円曲線については（A）（B）が成立する」とまとめられる。これに関連して次の有名な予想がある。

（C） **Shimura-Taniyama-Weil 予想.** すべての $\mathbf{Q}$ 上の楕円曲線は modular 楕円曲線である。

この予想が証明されればすべての $E/\mathbf{Q}$ について（A）（B）が成り立つ事になる訳である。（ N が平方因子を含まない場合に、Wiles によって（C）が証明された様である。）

4. BSD予想

前節と同様に $E/\mathbf{Q}$ を考えよう。有理点の群 $E(\mathbf{Q})$ について次の定理がある。

Theorem 4 (Mordell (-Weil)). $E(\mathbf{Q})$ は有限生成アーベル群である。

Theorem 4 により、

$$E(\mathbf{Q}) \cong E(\mathbf{Q})_{tor} \oplus \mathbf{Z}^r \qquad (r \geq 0)$$

と表せる（ $E(\mathbf{Q})_{tor}$ は位数有限の元全体）。この r を $r(E/\mathbf{Q})$ と書いて $E/\mathbf{Q}$ のランクと呼ぶ。

一方、予想（A）を認めると、$L(E/\mathbf{Q},s)$ は $s=1$ で正則であるから、そこでの位数（零点の order ）が考えられる。それを $\rho(E/\mathbf{Q})$ とおく（ $E/\mathbf{Q}$ の analytic rank ともいう）：

$$\rho(E/\mathbf{Q}) = \mathrm{ord}_{s=1} L(E/\mathbf{Q},s).$$

（何故これを考えるかについては6節を参照。）

この、$r = r(E/\mathbf{Q})$ と $\rho = \rho(E/\mathbf{Q})$ という一見無関係なものについて Birch と Swinnerton-Dyer は次の予想を立てた：

（D1）BSD予想. $r=\rho$ が成立する。

$r \leftrightarrow \rho$ には、「代数的 $\leftrightarrow$ 解析的」、「大域的なもの $\leftrightarrow$ 局所的なものの寄せ集め」という対比があるのでこれらが一致するというのは大胆な予想である。

さらに次の事も予想されている：

（D2）BSD予想.

$$\lim_{s\to 1} \frac{L(E/\mathbf{Q},s)}{(s-1)^{\rho}} = \frac{\Omega R |Ш(E/\mathbf{Q})| \prod_p c_p}{|E(\mathbf{Q})_{tor}|^2}$$

が成立する。

ここで右辺に登場する量の定義については文献を参照して頂きたい。一応、「知っている人には分かる」説明だけ与えておく。$\Omega = \int_{E(\mathbf{R})} |\omega|$ は周期であり、$c_p = [E(\mathbf{Q}_p) : E_0(\mathbf{Q}_p)]$ である。（ $p \nmid N \Longrightarrow c_p = 1$ となっている。）$R = \det(\hat{h}(P_i,P_j))_{1\le i,j\le r}$ は $E/\mathbf{Q}$ の regulator と呼ばれる実数である。ここで、$\hat{h}$ は $E/\mathbf{Q}$ の canonical height 、$P_1,\dots,P_r$ は $E(\mathbf{Q})/E(\mathbf{Q})_{tor}$ の（1組の）生成元を表す。また、

$$Ш(E/\mathbf{Q}) = \mathrm{Ker}(H^1(\mathbf{Q},E) \to \prod_{p\le\infty} H^1(\mathbf{Q}_p,E))$$

は $E/\mathbf{Q}$ の Tate-Shafarevich 群と呼ばれるアーベル群である。（ $H^1(K,E)$ はガロアコホモロジー群 $H^1(\mathrm{Gal}(\overline{K}/K),E(\overline{K}))$ の事で、$H^1(\mathbf{Q},E) \to H^1(\mathbf{Q}_p,E)$ は埋め込み $\mathbf{Q} \to \mathbf{Q}_p$ から定まる自然な写像である。ここで $\mathbf{Q}_\infty = \mathbf{R}$ としている。）

$Ш(E/\mathbf{Q})$ については次の予想がある。

（E）. $Ш(E/\mathbf{Q})$ は有限群である。

（D2）は（E）を前提とした予想である。Rubin と Kolyvagin によって、ある種の $E/\mathbf{Q}$ について（E）が成立する事が示されたものの、一般には未解決である。$Ш(E/\mathbf{Q})$ が有限群なら $|Ш(E/\mathbf{Q})|$ は平方数である事が分かっている。

BSD予想（（D1）と（D2））については Birch, Swinnerton-Dyer, Cassels, Coates-Wiles, Greenberg, Gross-Zagier, Rubin, Kolyvagin その他の人々の多くの研究がある。これらについて詳しく触れるのは筆者には荷が重すぎるのでやめておく。（ Kolyvagin の仕事については青木氏による解説がある。）現在までに r （ または ρ ）が1以下の場合にはかなりの事が示されている（主に、Heegner point のおかげ）。しかし、r,ρ が2以上の時には今のところ決定的な結果はない。（筆者が知らないだけだったらごめんなさい。）新しいアイデア、手法が求められていると言っていいのではあるまいか。

5. 状況証拠

ＢＳＤ予想を支持する根拠については、予想の成立が確かめられている場合がある、という事の他に、いくつかの傍証（前向きの心証を与えるもの）があると思う。それらを、筆者の知っている範囲で挙げて見よう。

1：実例の計算.

ＢＳＤ予想（特に（Ｄ1））は、非常に多くの（$\mathbf{Q}$ 上の）楕円曲線に対して確かめられている。（（Ｄ2）については $|Ш(E/\mathbf{Q})|$ の”予測値”を取っている場合も含めて。）これは予想の強力な根拠といえよう。また、実例を計算する事は、単に予想を検証するためだけでなくむしろ逆に、予想の「生みの親」である、とも言える（6節を参照）ので、それだけ重要と言えよう。

2：同種（ isogeny ）による不変性.

E と E' を同種な（isogenous）楕円曲線とする（つまり、全射 $\varphi : E \to E'$が存在する）時、E について（Ｄ1）、（Ｄ2）が成立する事と、E' について（Ｄ1）、（Ｄ2）が成立する事とは同値になる。（（Ｄ1）については難しい事ではない。難しいのは（Ｄ2）の右辺が同種により不変な事で、これは Cassels による。）（Ｄ2）の右辺に出てくる個々の量は同種により変化してしまうので、Cassels の結果は予想（Ｄ2）が「うまくできている」ことを示すものと言えよう。

3：0次元の場合の類似.

Fを有限次代数体とする。Fについての良く知られた古典的事実（下の Theorem 5 ）はＢＳＤ予想の「類似」と見なせるだろう。（ $E(\mathbf{Q})$（楕円曲線の場合）と E_F（代数体の場合）を「似ている」と思おう。）実際、K 群を使えば、これらは大きな予想の特別な場合と解釈される。

少し記号を説明しよう。O_F を F の（極大）整数環とし、$E_F = O_F^{\times}$ を F の単数群とする。また、

$$\zeta_F(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$$

を F のデデキントゼータ関数とする（ $\mathfrak{a}$ および $\mathfrak{p}$ は各々 O_F のイデアル、素イデアル全体を動き、$N(\mathfrak{a})$ はそのノルム）。r_1, r_2を各々 F の実素点、虚素点の数として、$r = r_1 + r_2 - 1$とする。また、$(E_F)_{tor}$ は F 内の1のべき根の群を表し、$w = |(E_F)_{tor}|$ である。h, R は各々 F の類数と regulator である。

Theorem 5.

(1)

$$E_F \cong (E_F)_{tor} \oplus \mathbf{Z}^r.$$

(2)

$$\mathrm{ord}_{s=0}\, \zeta_F(s) = r.$$

(3)

$$\lim_{s \to 0} \frac{\zeta_F(s)}{s^r} = -\frac{Rh}{w}$$

4 : Geometric Analogue.

$\mathbf{Q}$ の代わりに、$\mathbf{F}_q$（q は素数のべき）上の1変数代数関数体 K を取ってみる。K と代数体との類似は良く知られているので、K 上の楕円曲線 E/K について（D1）、（D2）、（E）に当たる予想（BSD予想の Geometric Analogue）が考えられている。（それらを、$(\mathrm{D}1)_{\mathrm{geom}}$ 等と表す。）M.Artin, Tate, Milne などの仕事によって次の事が知られている（詳しい事は省略）:

(1) $p \neq 2$ なら、「$(\mathrm{D}1)_{\mathrm{geom}} \Longrightarrow (\mathrm{D}2)_{\mathrm{geom}}$ 及び $(\mathrm{E})_{\mathrm{geom}}$」が成立。
(2) いろいろなケースについて、$(\mathrm{D}1)_{\mathrm{geom}}$ の成立が分かっている。

証明には、E 自身を $\mathbf{F}_q$ 上の「曲面」と見なす、という態度が重要である。これが「geometric」の意味であり、$\mathbf{Q}$ 上の場合にはできなかった芸当である。この Geometric Analogue も、（代数体と代数関数体の類似に鑑みて）BSD予想を（心理的に）支持する根拠と言えるだろう。

6. 予想の由来

BSD予想は（現在では）正確に定式化された主張であるから、その内容について論理的には疑問の余地はない。あとは成り立つかどうかを追求するのみである、とも言えるだろう。しかし、考えて見ると、$\rho(E/\mathbf{Q})$ は $L(E/\mathbf{Q}, s)$ の「収束するかどうかも分からない」点での位数（まあ、[CM] や [MOD] の場合には大丈夫だが）であるし、（D2）の右辺においては、$|Ш(E/\mathbf{Q})|$ は「有限かどうかも分からない」数である。（予想ができた段階では Rubin, Kolyvagin の結果はなかった。）だから、BSD予想に最初に触れた人は、「何でこんな事を考えたのか？」という心理的疑問を持つに違いない。そこで最後に、BSD予想が生まれた背景について少し触れたい。と言っても、筆者が Birch 氏や、Swinnerton-Dyer 氏から直接何か聞いたわけではなく、原論文にちゃんと書いてある事を説明するだけであるが。（内輪話を知っている方は教えて下さい。）以下は主に、Birch and Swinnerton-Dyer : "Notes on elliptic curves II", Crelle 218 (1965) pp.79–108 による。

先ず2次形式に関する Siegel の結果がある。（Siegel の定理は非常に一般的なものだが、簡単のため）整数係数の正定値2次形式 $Q(x_1, \ldots, x_n)$ と $t \in \mathbf{N}$ を考える。素数 p に対して $Q(x_1, \ldots, x_n) \equiv t \pmod{p}$ の $x_1, \ldots, x_n \in \mathbf{F}_p$ なる解の個数を N_p とする。そこで Siegel の定理は、

$$\lim_{x \to \infty} \prod_{p \leq x} \frac{N_p}{p^{n-1}}$$

が有限であり、その値を具体的に表せる事を主張する。（実際にはもっと微妙な定式化が必要であり、また表示の仕方が大切だが、すべて省略する。）

さて、3次の場合がどうかと考えると、$\mathbf{Q}$ 上の楕円曲線を考えて見る事になる。（上記の論文においては、(*) で $B = 0$ となる場合（[CM] のケース）を考えている。）この時、Siegel の場合と同様に

$$f(x) = \prod_{p \leq x} \frac{N_p}{p}$$

を調べてみる。（N_p は E の $\mathbf{F}_p$− 有理点の個数。(**) を考えれば良いから $n = 2$ 。）しかし、この場合は2次形式の場合と違って、多くの実例について $f(x)$ は $x \to \infty$ で発散しているようだと分かる。しかし、ここでやめてしまわないのが偉い。$f(x)$ の発散の仕

方を見てみると、$x \to \infty$ で

$$f(x) \sim c(\log(x))^g \qquad (g \geq 0 \text{ は整数で、} c \text{ はある定数})$$

となっているようだと分かる。(実際は $f(x)$ はかなり振動しているそうですが。) この g の値は E ごとに変わるのだが、それが $E(\mathbf{Q})$ のランク (これは別に計算してある) に一致するらしいと見当をつけるのである。(すごい!) あとは、$E \pmod p$ が good reduction である時は

$$\frac{N_p}{p} = (1 - a_p p^{-s} + p^{1-2s})\big|_{s=1}$$

という事に注意して、「$f(x)$ の発散の仕方」を「$L(E/\mathbf{Q}, s)$ の $s = 1$ での位数」に言い換えれば予想 (D 1) ができるのである。(D 2) の右辺の値についても、多くの実例を計算し、また理論的考察も加えながら「試行錯誤で」求めていくのである。($|Ш(E/\mathbf{Q})|$ については、いつでも有限だ、とは結論できないものの、値 (特に 2− part) の見当はつくのである。) この辺りの詳細は述べない (述べられない) が、とにかくすごい迫力である。(筆者の解説などではなく) 原論文を読まれる事をお勧めして、この記事を終える事にする。