数理解析研究所講究録
971巻 1996年 30-39

楕円曲線の数論の歴史

早稲田大学　足立恒雄 (Adachi, N.)

本稿は津田塾大学で開催されたシンポジウム『20世紀数学』（'95年11月）における講演と京大数理解析研究所における研究集会『代数的整数論とフェルマー問題』（'95年12月）における講演をまとめ、加筆修正したものである。

楕円曲線の歴史と一口に言っても膨大・多岐に亙るから、ここでは(1)Fermatの先駆的研究、(2)楕円曲線の群構造発見を巡る歴史、(3)フェルマー問題のFreyによる谷山予想への還元、の三つに絞って考察することにする。

§1 楕円曲線論先史

Diophantos(AD 3C, [3])は『算術』と呼ばれる著書13巻を著した。その内容は2次曲線上の有理点を求めることを要求する問題集で、現在では6巻までが遺されている。『算術』で扱われている例をいくつか下に挙げる：

例1-1　与えられた平方数を二つの平方数の和に分けよ。例えば、

$$x^2 + y^2 = 4^2$$

の（有理）解を求めよ。

例1-2　与えられた数が二つの平方数の和であるとき、これを別の二つの平方数の和に分けよ。例えば、$13 = 2^2 + 3^2$ を知って

$$13 = x^2 + y^2$$

の別の（有理）解を求めよ。

例1-3　2連方程式

$$a_1x + b_1 = \square, \quad a_2x + b_2 = \square$$

例えば、

$$x + 2 = \square, \quad x + 3 = \square$$

の（有理）解を求めよ。

Diophantosの扱った非特異3次曲線は

$$y^2 = x^3 \pm 2$$

の二つだけで、これはたまたま解がうまく見つかった場合であったといえる。3次曲線に対する、Fermatの言うBachetの方法（接弦法）にあたる手法の適用はみられない。WeilなどがDiophantosを接弦法の始祖のようにいうのは読み込みすぎではなかろうか。

Diophantos の『算術』は、上の例でわかるように、問題は整数係数で与えられているとしても、もっぱら「有理数解」を求めた著作で、整数解が見つからない場合に、やむなく有理数解を求めているというのではないことは注目に値する。

なお、最近見つかった『算術』の一部（アラビア語テキスト、9 世紀頃の写本と考えられる：テキストならびに英訳は [25]）には 3 次以上の方程式が頻出するが、非特異 3 次曲線の問題に還元されるものは見当たらない。従って、散逸した『算術』の諸巻にはさらに高度な問題が扱われていたという可能性は薄いだろう。アラビア語版テキストが真正の『算術』であるかどうか、いくらか疑問の余地もあるが、いずれにしても、不定方程式の伝統がアラビアに受け継がれていたことははっきりしている。

§2 楕円曲線論の始祖 Fermat

Fermat が著した有理点に関する著作は、ギリシャ語原点から Bachet が訳した『算術』の余白に書き込んだ《Observationes（欄外書き込み集）》([4]) の他に、心酔者である神父 Jacques de Billy に書かせた《Doctrinae Analyticae Inventum Novum》([5] ; Inv. Nov. と略記する) がある。この Inv. Nov. は全編、楕円曲線上の有理点の考察に当てられた長大な論文である。Fermat の扱った例をいくつか挙げてみよう。

例 2-1(Obs. 3) 二つの立方数の和である数を他の二つの立方数の和に表せ：

$$x^3 + y^3 = a \neq 0$$

の解が一つ与えられたとき他の解を無数に求めよ。

例 2-2(Obs. 45) （有理）数を 3 辺とする直角三角形の面積は平方数ではありえない：

$$x^2 + 1 = \square, \quad x^2 - 1 = \square$$

は解を持たない。

例 2-3(Obs. 16) 3 連方程式

$$x + 1 = \square, \quad 3x + 1 = \square, \quad 8x + 1 = \square$$

の解を求めよ。

例 2-4(Inv. Nov., Pt.1, 15)　2 連方程式

$$x^2 + x + 2 = \square, \quad x^2 + 3x + 3 = \square$$

の（$x = -2$ 以外の）解を求めよ。

例 2-5(Inv. Nv. Pt.3, 12) 不定方程式

$$x^4 + 4x^3 + 10x^2 + 20x + 1 = \square$$

の（$x = -3$ 以外の）解を求めよ。

Ex 6(Inv. Nov., Pt. 2, 11) 3 連方程式

$$x + 1 = \square,\ \ 2x + 1 = \square,\ \ 3x + 1 = \square$$

は（$x = 0$ 以外に）解を持たないことを示せ。

Ex 7(Inv. Nov., Pt. 2, 10) 3 連方程式

$$5x + 1 = \square,\ \ 16x + 1 = \square,\ \ 21x + 1 = \square$$

は無数に解を持つ。

楕円曲線 E 上の有理点 P が与えられたときに、点 P における接線が再び E と交わる点を求めることによって E の新しい有理点を得る方法を Fermat は Bachet の方法と呼んでいる（我々は接弦法とも呼ぶことにする）。従って、これは Fermat の独創ではないが、数々の問題に適用して楕円曲線の数論と言える理論にまで発展させたのは、間違いなく Fermat の功績である。

上掲の諸例はすべて、$x = 0$（あるいは x を $1/x$ と変数変換して $x = 0$ としたもの）を与えられた有理点として持っている。しかし、Fermat は 0 を数とは見なしていなかった。また、例 2-4,2-5 は負の数が予め解として与えられているが、負数もこの時代には数と認められていなかった。従って、Fermat は意識してはいなかったとしても、現代の目からみれば Fermat の扱った問題はすべて、視察で容易にわかる有理点を持つ楕円曲線上に有理点が無数にあるか否かを問う問題であったことがわかる。

Fermat の扱った 3 連方程式は

$$Ax + 1 = \square,\ \ Bx + 1 = \square,\ \ Cx + 1 = \square \tag{1}$$

という形にまとめることができる。まず

$$x = Ay^2 + 2y$$

と置いて、(1) の第 1 式に代入すれば、左辺は平方数となる。そこで第 2、第 3 の式を解けば良いことになるが、それは

$$ABy^2 + 2By + 1 = u^2,\ \ ACy^2 + 2Cy + 1 = v^2 \tag{2}$$

である。これは例 2-4 で出てきた 2 連方程式である。(2) の 2 式の差を作ると、

$$(B - C)y(Ay + 2) = u^2 - v^2 = (u + v)(u - v)$$

となる。そこで

$$u+v=(B-C)y,\quad u-v=Ay+2$$

として、u,v を求めるというのが、2連、従って3連方程式を解く Fermat の方法である。この方法によれば、

$$u=\frac{A+B-C}{2}y+1$$

であるから、

$$A+B=C \tag{3}$$

の場合にはうまくいかない。上掲の、例2-6,2-7の場合がそれに当たる。このうち、2-6には解がないことの証明を持っていると Fermat は主張している(が、その証明は残されていない)。しかるに、2-7は無数に解を持つと指摘している。このように、Fermat は、今でいう楕円曲線の有理点問題に関心を持ち、深い研究をしていたのであった。

(3) の場合に Fermat の方法が何故うまくいかないのかは Zagier([37]) により解明された。まず、よく知られているように、曲線 (1) は

$$y^2=(Ax+1)(Bx+1)(Cx+1) \tag{4}$$

と双有理同値である。楕円曲線 (4) 上には自明な有理点 $P(0,1)$ がある。また、$x=-1/A$, $-1/B,-1/C$ に対応する点は位数2を持つ有理点である。Mazur の定理 ([18]) を適用すると、点 P が有理 torsion であるための必要十分条件が簡単に出てくる。全部で4つあるその条件の一つが (3) というわけである：その他の条件は $\sqrt{A}+\sqrt{B}=\sqrt{C}$ など、無理式で与えられる。もちろん、点 P が torsion 点であっても、他に無限位数を持つ有理点が存在する場合がありえるわけで、その1例が例2-7である。

なお、Fermat は FLT の $n=4$ の場合、即ち

$$x^4+y^4=z^4$$

には自明でない解が存在しないことを証明している。この曲線の種数は3であるけれども、実際には

$$x^4+y^4=z^2$$

という種数1の曲線に問題を還元して解いているわけで、あの「悪夢のような一瞬」を除けば、一度たりとも種数1という守備範囲から逸脱した考察をしたことはなかったという Weil の指摘は説得的である。

§3 群構造の発見

種数1の曲線と楕円関数との関係に初めて気が付いたのは Jacobi ([15]) であろう。Euler の残した4次曲線の有理点問題、つまり、例えば例2-5のような曲線上に、一つ有理点が与えられたとき、次々と他の有理点を求める問題を楕円関数を使って（具体的に解いてみせたわけではないが）一般的に解く原理を説明したのである。この論文の最後に、こ

ういった原理がEulerを初めとする楕円積分の開拓者にわからなかったはずはないと指摘しているが、実際にはEulerは不定方程式論と曲線論、積分論を結び付けて考えたことは一度もなかったのである。

代数曲線の解析関数によるパラメトリゼーションを研究したのはClebschが最初である。例えば、種数1（この名称もClebschによる）の曲線が楕円関数によってパラメトライズされることを示した([1])。これを使って、例えば3次曲線の変曲点の個数や、3点の共線条件など、古典幾何学の数多くの問題が解かれた。

Poincaréは代数体上定義された代数曲線の有理点の集合について考察した。論文[23]では楕円関数によるパラメトリゼーションを使って、パラメータ$u_1, \ldots, u_n$から基本操作（接弦法）を繰り返して得られる点は

$$\sum_{i=1}^{n} x_i u_i, \quad \sum_{i=1}^{n} x_i \equiv 1 \pmod 3$$

であると主張している。同じことが（n=3の場合に）Hurwitz([13])によっても指摘されている。この表示法を見てもわかるように、ここには楕円曲線が群をなすという意識はまだ見られない。一点Oを定めて、このOを中心として対称点を取るという操作（パラメータでいえば、uに$-u$を対応させる操作）を基本操作に含めることを除外しているのが、群構造に気付かれなかった理由のように思われる。Poincaréは点の個数nを増やしていけば、すべての有理点が尽くされるようにできると暗黙のうちに認められていて、そういうnの最小数を階数というと定義している。

Hurwitz([14])はPoincaréと同じ考察から始め、特に、有理点の集合$E(\mathbf{Q})$が有限の場合を扱っている。この際には、「演算が閉じているので$E(\mathbf{Q})$は群をなす」ということが明白に指摘されている。また有理点を持つ3次曲線は座標変換によってWeierstrassの標準形に直せることも述べられている。このことを使って、

$$x^3 + ay^3 + bz^3 = 0$$

という型の不定方程式に関する結果から、$E(\mathbf{Q})$の位数が$2, 3, 4$となる楕円曲線を与えている。

Levi([16])はOgg予想とも呼ばれた、torsion部分の群の位数に関する命題を既に予想しているというが、筆者は未見である。

Haentzschel([9]他)はFermat以来の楕円曲線の有理点問題、例えば

$$y^2 = 4(x+8)(x^2 - 8x + 43)$$

に初めてWeierstrassの$\wp$関数を応用した。これが具体的な数論の問題に楕円関数が応用された最初であろう。

なお、Schlesinger [35]は以上述べてきた、Fermat, Euler, Jacobi, Poincaréの仕事を手際よく紹介した、最も早い時期の解説記事である。

Mordell([21])は群$E(\mathbf{Q})$が有限生成であるという、いわゆるPoincaré予想を証明した。しかし、この表現は今風で、彼自身はPoincaréや、それを紹介したSchlesinger同様、「有

限個の点から接弦法によってすべての有理点が得られる」と表現している。Mordell は

$$y^2 = Ax^4 + Bx^3 + Cx^2 + Dx + E$$

に整数解が有限個しか存在しないことを証明しようとして失敗し、その過程を振り返っているうちに Finite Basis Theorem の証明ができているのに気付いたのだという（[32]）。その結果を 3 次の非特異曲線の結果に述べ直したのである。4 次曲線に代数的数論を適用したその証明の概略は [33] に紹介されている。

論文 [21] には、加群というような用語は現れないけれども、既に有限個のパラメータ $u_1, ..., u_n$ が取れてすべての有理点が

$$m_1u_1 + ... + m_nu_n, \quad m_j \in \mathbf{Z}$$

という形に書けるという表現になっている。これによって、Mordell、あるいは Hurwitz と Mordell の間のころに、少なくとも implicit には楕円曲線上の点の全体が群をなすという事実が気付かれたものと思われる。

Weil([29]) は Finite Basis Theorem の証明を簡易化したが、パラメータの加法演算の幾何学的な意味も説明し、目的が「この加群が有限生成であることの証明である」と宣言している。また、その証明も（Mordell の場合と違って）群であるという事実が基本的に使われている。このようなわけだから、楕円曲線の群構造を explicit に指摘した人は **Weil** であるといって良いことになるのではなかろうか。

§4 Frey の貢献

Wiles による FLT の最終決着に至る道を考えるとき、最も crucial な turningpoint は Frey 曲線の導入と FLT の谷山予想への還元であろう（[8]）。どうして Frey はこの奇妙なアイデアにたどりついたのか、その経緯を探るのが本節の主題である。

70 年代の初め頃、楕円曲線の torsion 点の決定問題の研究が盛んであった。Néron の還元理論 ([22]) を応用すると、楕円曲線が有理的 torsion を持つための局所条件が出てくる。これらの条件を調べると、必然的に Fermat 方程式に類似の不定方程式が登場する。例えば、

定理 (Demjanenko [2], Hellegouarch [12]) 楕円曲線 $E(\mathbf{Q})$ が位数 p^2 の有理点を持てば、Fermat 方程式

$$x^p + y^p = z^p, \quad xyz \neq 0$$

は $p \mid xyz$ なる整数解を持つ。従って、p が正則素数ならば、$E(\mathbf{Q})$ は位数 p^2 の点を持ち得ない。

Frey はいくらか遅れて torsion 部分群決定のゲームに参加し、上の定理と似たような定理をいくつか証明した ([6]) : この、遅れて参加したことが FLT 解決のためには幸いした

のである。Frey がこの論文を出したのと奇しくも同じ年、Mazur([17], [18]) が有理 torsion 問題における最終結論に到達した。こうした場合、Frey の仕事はほとんど無に帰することになるのが普通である（実際、[6] には校正時に挿入した脚注として、「こうした定理の仮定は決して満たされないことが Mazur によって証明された」と記されている）。ところが、この論文の中に 1 ページだけ、後になって重要な意味を持つ考察がされていた。つまり、問題の逆が考察の対象になっているのである：

> 自然に逆の問題が持ち上がる：上の方程式に解があるならば、位数 p の有理点を持つような楕円曲線が存在するだろうか？

Frey は続いて、「そうした有理点が存在するか、さもなければガロア群が体 K が存在する」ということを証明している。これには p-torsion points の座標の添加によって、ほとんどの場合、$GL_2(\mathbf{F}_p)$ をガロア群に持つ体が生成されるという Serre([26]) の結果が使われている。Mazur の結果によれば、「そうした有理点は存在しない」のであるから、「ガロア群が $GL_2(\mathbf{F}_p)$ に同型で $\mathbf{Q}(\zeta_p)$ 上不分岐な体が存在する」ことになる。この考察のおかげで、Frey にとっては Mazur の結果は問題の終焉ではなく、新しい問題の始まりであった。

modular curve との関連は Frey[7] において初めて登場する。この論文では moduli problem を考えることによって、Fermat curve に対する Mordell 予想（今や、Faltings の定理）と modular curve との関連が研究されている。結果自身は大したものではないが、この中で、いわゆる Frey curve

$$y^2 = x(x - a^p)(x - c^p)$$

（ここに a,b,c は

$$a^p + b^p = c^p$$

を満たす自然数）の持っている不可思議な性質、例えば、semi-stable であること、判別式が 2 の因子を除けば $2p$ 乗数であること、先に述べたような小さな分岐を持つ大きなガロア拡大が存在すること等が列挙されている。この Frey curve の異様性が Frey に FLT は正しいに違いないという確信を持たせるに至ったのである。

谷山予想への還元の経過を Frey 自身の見方でまとめてみると次のようになる：

> (Frey に問い合わせた筆者に対する手紙の要旨) Mazur の重要な仕事を契機として二つのことが新しくわかった。第一は、p-torsion points の座標を添加することによって $GL_2(\mathbf{F}_p)$ と同型なガロア群を持つ体が生成され、その分岐は楕円曲線の算術によって制御されるのだが、それまでの考察を逆に辿ることによって、Fermat 型の方程式の解がたいへん小さな分岐を持つ大きな拡大体を与えることになることである。ガロア群が $GL_2(\mathbf{F}_p)$ で、$2p$ において小さな分岐を持つだけの体の存在 (ないしは非存在) の問題は Kummer による正則素数の判定の 2 次元版とみなせる。第二に、modular form の算術と関係があるという事実である。これが本質的な部分である。

1984年、FreyはOberwolfachで

$$\text{谷山予想} \Longrightarrow \text{FLT}$$

という予想をし、証明のためのアイデアを説明した。このアイデアは公刊されなかったが、「Eの Néron model を考察し、bad reduction を持つ素点での mod p reduction での component の個数を modular curve $X_0(N)$ の Jacobian の同様な個数と比較して、これらが一致しないことから、任意の楕円曲線が modular curve でパラメトライズされるという仮定に矛盾する」という筋書が[34]の中で簡単に解説されている。数カ月後、Serre はより簡潔な、Galois 表現を利用した形に改良し、実際には

$$\text{谷山} + \epsilon \Longrightarrow \text{FLT}$$

であるとして、その ϵ を次のように定式化した：

Epsilon Conjecture([27])

(1) ρ を level $pM, (p, M) = 1$, かつ weight 2 の modular representation とし、ρ は p で finite であるとする。このとき ρ は実は level M, weight 2 の modular representation である。

(2) ρ を level $M_1M_2, (M_1, pM_2) = 1$, weight 2 の modular reresentation とし、さらに ρ は M_1 の素因子で不分岐とすると、実は ρ は level M_2, weight 2 の modular representation である。

Frey はこうした Serre の助けをまとめて論文[8]とした（1986）。Frey 以後の展開については[34]が簡潔で、要を得ていてよい。ϵ Conjecture は Mazur[19] によって部分的に、その手法を一般化させて Ribet[24] によって完全に、証明された。

参考文献

[1] Clebsch, A., *Über diejenigen Curven, deren Coordinaten sich als elliptische Funktionen eines Parameters darstellen lassen*, J. Reine Angew. Math. 64, 210-270, 1865

[2] Demjanenko, V. A., *Points of finite order on elliptic curves* (Russian), Acta Arith. 19, 185-194, 1971

[3] Diophantus, *Diophante d'Alexandrie* (tr. by P. V. Eecke), Blanchard, Paris, 1959

[4] Fermat, P. de, *Oservationes*, Oeuvres de Fermat, tome 3, 241-274, Gauthier-Villars, 1896

[5] —, *Doctrinae Analyticae Inventum Novum*, ibid., 325-398

[6] Frey, G., *Some remarks concerning points of finite order on elliptic curves over global fields*, Arkiv. Mat. 15, no.1, 1-19, 1977

[7] —, *Rationale Punkte auf Fermatkurven und getwisteten Modulkurven*, J. Reine Angew. Math. 186-191, 1982

[8] —, *Links between stable elliptic curves and Diophantine equations*, Annales Universitatis Saraviensis, Series Mathematicae, 1, 1-40, 1986

[9] Haentzschel, E., *Euler und die Weierstraßsche Theorie der elliptischen Funktionen*, Jahresbericht d. Deutschen Math.-Vereinigung, 22, 1913, 278-284

[10] Hellegouarch, Y., *Étude des points d'ordre fini des variétés abéliennes de dimension un définies sur un anneau principal* , J. Reine Angew. Math. 244, 20-36 (1970)

[11] —, *Courbes élliptiques et équation de Fermat*, Thèse, Besançon, 1972

[12] —, *Points d'ordre $2p^h$ sur les courbes élliptiques*, Acta Arith. 26, 253-263, 1975

[13] Hurwitz, A., *Über die Schröter'sche Konstruktion der ebenen Kurven dritter Ordnung*, J. Reine Angew. Math., Bd. 107, 141-147, 1891 = Werke, Bd. II, 722-728

[14] —, *Über ternäre diophantische Gleichungen dritten Grades*, Vierteljahrschrift d. Naturfor. Gesell. Zürich, 62, 1917, 207-229 =Werke, II, 446-468

[15] Jacobi, C. G., *De usu theoriae integralium ellipticorum et integralium abelianarum in analysi diophantea*, J. Reine Angew. Math. 13, 353-355, 1834 = Gesammelte Werke II, 51-55

[16] Levi, B., *Saggio per una teoria aritmetica della forme cubiche ternarie*, Academia reale delle scienze di Torino, Nota I-IV, 1906-1908

[17] Mazur, B., *Modular Functions of One Variable I*, Springer LN 320, 1977

[18] —, *Modular curves and the Eisenstein ideal*, IHES 47, 33-186, 1977

[19] —, *Letter to J-F. Mestre*(16 August 1985)

[20] Mordell, L. J., *On the rarional solutions of the indeterminate equations of the third and fourth degrees*, Proc. Camb. Phil. Soc., 21, 179-192, 1922

[21] —, *Indeterminate equations of the third and fourth degrees*, Quart. J. Pure and Applied Math., 45, 170-186, 1914

[22] Néron, A., *Modéles minimaux des variétés abéliennes sur les corps locaux et globaux*, IHES 21, 1974

[23] Poincaré, H., *Sur les propriétés arithmétiques des courbes algébriques*, J. Math.(3), 7(1901), 161-233 = Oeuvres, V, 483-548

[24] Ribet, K., *On modular representations of Gal($\bar{\mathbf{Q}}/\mathbf{Q}$) arising from modular forms*, Inv. Math. 100, 431-476, 1990

[25] Sesiano, J., *Books IV to VII of Diophantus' Arithmetica*, Springer, 1982

[26] Serre, J-P., *Propriété galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math. 15, 259-331, 1972

[27] —, *Lettre à J-F. Mestre(13 août 1985)*, Contemp. Math. 67, 263-268, 1987

[28] —,*Sur les représentations modulaires de degré 2 de Gal($\bar{\mathbf{Q}}/\mathbf{Q}$)*, Duke Math. J. 54, 179-230, 1987

[29] Weil, A., *Sur un théorème de Mordell*, Bull. Sci. Math., (2) 54 (1930), 182-191 = Collected Papers, 1,

* * *

[30] Dickson, L. E., *History of the Theory of Numbers*, vol. 2, Carnegie Institute of Washington, 1920 (reprint, Chelsea, 1971)

[31] Dieudonné, J. (ed.), *Abrégé D'histoire des mathématiques*, 2 vols, Herman, Paris, 1978

[32] Mordell, L. J., *A Chapter in the Theory of Numbers*, Cambridge, 1947

[33] —, *Diophantine Equations*, Academic Press, 1969

[34] , Ribet, K. A., *Galois representations and modular forms*, Bull. AMS (New Series), 32(4), 375-402, 1995

[35] Schlesinger, L., *Über ein Problem der diophantischen Analysis bei Fermat, Euler, Jacobi und Poincaré*, Jahresbericht, 17, 57-67, 1908

[36] Weil, A., *Number Theory: An Approach through History; From Hammurapi to Legendre*, Birkhäuser, 1983

[37] Zagier, D., *Elliptische Kurven: Fortschritte und Anwendungen*, Jber. d. Dt. Math.-Verein., 92, 58-76, 1990