数理解析研究所講究録
第157巻 1972年 19-28

楕円曲線のconductor

名大 理　　谷野敏博

1. Cを有理数体$\mathbb{Q}$上定義された，しかもそのglobal minimal Weierstrass modelとして平面三次曲線

$$y^2+a_1xy+a_3y+x^3+a_2x^2+a_4x+a_6=0 \qquad a_i\in\mathbb{Z}$$

をとる楕円曲線即ち一次元Abel多様体とする。 Weilに従い，Cのconductor Nを

$$N=\prod_{\text{all prime } p} p^{(\mathrm{ord}_p\Delta+1-n_p)}$$

で定義する。ここでΔはCの判別式，n_pは重複度を考えないNéron fibreの成分の個数とする。Nのp-exponentはCのpによるreductionに応じて，

$$\mathrm{ord}_p\Delta+1-n_p=\begin{cases} 0 & \text{for non-degenerate reduction} \\ 1 & \text{for multiplicative ——} \\ 2 & \text{for additive —— \& } p\neq 2,3 \\ \geq 2 & \text{for additive —— \& } p=2,3 \end{cases}$$

となり，しかもCはどこかでdegenerate reductionをもつ. i.e. $N\neq 1$

であることが Tate, Ogg により知られている [16]。 また, C_ℓ を order ℓ の点の群とするとき, Serre による ramification の measure $\delta(\mathbb{Q}_p, C_\ell) = \delta_p$ ($p \neq \ell$, これは ℓ に依らない [16]) と reduction が non-degenerate, multiplicative, additive に応じて $\varepsilon_p = 0, 1, 2$ とおいた ε_p を用いて

$$\mathrm{ord}_p \Delta + 1 - n_p = \delta_p + \varepsilon_p$$

となる。高次元 Abel 多様体の conductor についても, この δ を用いて同様に定義されている ([17] 参照)。

さて, 与えられた conductor N をもつ楕円曲線の決定という問題を考えてみる。これは一般には困難な問題で, 判別式の形から essential に diophantus 方程式 $y^2 = x^3 + k$ の有理数解の考察に帰することもできる。Thue の定理から, だからそんな曲線は有限個である。Ogg は $N = 2^\lambda, 3\cdot 2^\lambda, 9\cdot 2^\lambda$ のとき, そんな曲線は order 2 の有理点をもつことを示すことにより, 全ての曲線を決定した。その後 Coghlan は $N = 2^m 3^n$ を扱った。つまり Ogg [14] [15] に依れば曲線が order 2 の有理点をもてば (以下 $C_{\mathbb{Q},2} \neq 0$ と書こう), あとは diophantus 方程式の取扱いだけになる。このことに注意して以下 $N = 2^m p^n$ ($p \neq 3$, odd prime) の曲線を扱う。

2. C の 2 分点を $\mathbb{Q}$ と付加した体 $K = \mathbb{Q}(C_2)$ の $\mathbb{Q}$ 上の

pでの分岐指数をe_pと書くとき，Ogg [15] 2. と同様な考察で，2次体 $\mathbb{Q}(\sqrt{\pm p})$，$\mathbb{Q}(\sqrt{\pm 2p})$ のすべての類数が3で割り切れないような odd prime p に対して，$N = p\cdot 2^\lambda$ で $e_2 = 1$ or 2 ならば $C_{\mathbb{Q},2} \neq 0$ を得る．とくに $\lambda = 1$ のときは Tate の理論により必然的に $C_{\mathbb{Q},2} \neq 0$ となる．Ogg 及び後に独立して Neumann [12] は $N = 2^\lambda$, $3\cdot 2^\lambda$, $9\cdot 2^\lambda$ のとき無条件に $C_{\mathbb{Q},2} \neq 0$ になることと示したわけである。他のpに対しては次のことが示される，即ち

命題 $p \equiv 1$ or $7 \pmod 8$ で $3 \nmid h(\mathbb{Q}(\sqrt{\pm p}))$ & $3 \nmid h(\mathbb{Q}(\sqrt{\pm 2p}))$ とするとき，$N = p\cdot 2^\lambda$ $(\lambda > 0)$ ならば $C_{\mathbb{Q},2} \neq 0$ である。例えば $p = 7$ がある．$p \equiv 3, 5 \pmod 8$ のときは diophantus 方程式 $y^2 = x^3 + k$ の考察が必要になるのでわからないが $p = 5$ などではこの命題にあたるものが云えそうである．しかし Ogg を拡張する次の定理が成立する：

定理1

$p \equiv 3$ or $5 \pmod 8$ で $3 \nmid h(\mathbb{Q}(\sqrt{\pm p}))$ かつ $3 \nmid h(\mathbb{Q}(\sqrt{\pm 2p}))$ とするとき，$N = 2p$ の楕円曲線は存在しない．

Ogg は [15] で実際 $N \neq 10, 22$ を示した．他のこのような p として 37, 43, 67, 197, 227 等がある．この証明は上の注意の $C_{\mathbb{Q},2} \neq 0$ が essential であり，次にあげる diophantus 方程式の結果(のいくつか)を必要とするが，方法は Ogg と同

様である。併し $p \equiv 1$ or $7 \pmod 8$ に対してはこの定理が成り立たないことはよく知られている。例えば $N=14$ の曲線は実際存在する (e.g. [6])。

3. ここでは $N = 2^m p^n$ ($p \neq 3$ は任意の odd prime) を扱う。1でみたように $n = 1$ or 2 である。(m, n は positive としている) 次の弱い結果を証明することができる。

定理2

$p \equiv 3$ or $5 \pmod 8$ で $N = 2^m p^n$ ($p \neq 3$, $m, n > 0$) のとき order 2 の有理点をもつ楕円曲線は Ankeny-Artin-Chowla の予想のもとで全て effective に決定される。とくに $p-2$ or $p-4$ が square のときはこの予想の仮定が取り除けるから $p = 3, 5, 11, 13, \cdots$ (*) に対しては全て effective に決まる。

(注) ここに云う Pell 方程式に関するよく知られた予想は $p \equiv 3 \pmod 4$ の時でも analogous な予想がある ([8] Chap. 8)。ここではもちろんそれも含んでいる。予想が確かめられている p についてはこの結果は有効である。"effective" という意味はもちろん曲線の方程式が具体的に好きなだけ求められるということである。

(*) $p = 3$ で $n = 1, 2$ が Oyama の結果である。

order 2 の有理点をもつ曲線は $y^2+x^3+a_2x^2+a_4x=0$, $a_i\in\mathbb{Z}$ minimal at all $p\neq 2$, 同時に $l^2|a_2$, $l^4|a_4$ とならないといった書き方ができ, しかも N を割る素因子と Δ を割る素因子は同一ということから $\Delta=2^4a_4^2(a_2^2-4a_4)=\pm 2^\mu p^\nu$ を満たす (a_2,a_4) が全てあげられれば, 後は Néron [11] の P.124-125 により (C-type の決定にはいささかめんどうなものがあるが) 定理2は証せられる。 この pairs (a_2,a_4) の決定には次の結果を用いる。

命題

(i) $X^2-1=2^\alpha p^\beta$ の整数解は $p\equiv 3$ or $5\pmod 8$ のとき, trivial な $\alpha\beta=0$ も含めて $(|X|, 2^\alpha p^\beta)=(2,3),(3,2^3),(5,2^33),(7,2^43),(9,2^45),(17,2^53^2)$ に限り, $p\equiv 1$ or $7\pmod 8$ のとき non-trivial な解は $\beta=1$ で $p=2^{\alpha-2}\pm 1$ $(\alpha\geq 5)$ で与えられる。

(ii) $X^2+1=2^\alpha p^\beta$ の non-zero 整数解は $p\equiv 3\pmod 4$ のとき, trivial な解 $|X|=1$ に限り, $p\equiv 1\pmod 4$ のとき, 更に $\alpha=0$, $\beta=1$又は $\alpha=1$, $\beta=1,2$ or 4 になる。とくに $\beta=4$ になるのは $p=13$, $|X|=239$ だけである。

(iii) $2X^2+1=p^\alpha$ $(\alpha>0)$ の整数解は $p\equiv 7$ or $5\pmod 8$ のとき存在しない。$p\equiv 1$ or $3\pmod 8$ のとき, $(|X|,p^\alpha)=(11,3^5)$ を除いて $\alpha=1$ or 2 になる。

(iv) $2X^2-1=p^\alpha$ $(\alpha>0)$ の整数解は $p\equiv 3$ or $5 \pmod 8$ のとき存在しない。

(v) $|\pm p^\alpha - X^2| = 2^\beta$ の整数解は trivial な $(\pm p^\alpha, |X|) = (1,3), (-1,1)$ を除いて，Ankeny-Artin-Chowla の予想とその analogy の成り立つ p に対して，$p\equiv 3 \pmod 8$ のとき，$\alpha=\beta=1$; $(\pm p^\alpha, |X|) = (3,2), (3^2,1), (3^3,5), (3^4,7), (-3,1)$ $(3^3,5)$, $p\equiv 5 \pmod 8$ のとき $\alpha=1, \beta=0$; $\alpha=1, \beta=2$; $(\pm p^\alpha, |X|) =$, $(5^2,3), (5^3,11)$ で与えられる。

(vi) $pX^2-y=\pm 2^\alpha$, $y=\pm 2^\beta$ の整数解は $2|X$, $4|y$ となるか，$p\equiv 3$ or $5 \pmod 8$ ならば，$p\neq 3,5$ では存在しないし，$p=3$ のとき $(x,y)=(1,4),(1,1),(1,2),(1,-1)$，$p=5$ のとき $(1,4),(1,1)$ に限るかである。

(注) (iv)-(vi) で $p\equiv 1$ or $7 \pmod 8$ に対しては容易でないが，このとき全整数解がわかれば all p に定理2は成り立つ。(v) で予想の部分は $X^2+2=p^\alpha$, $X^2+4=p^\alpha$ の考察から induce されているし，前者の不定方程式が予想の analogy に対応することは例えば Kutsuna [5] に依る。

命題は congruent な方法と $\mathbb{Z}[\sqrt{-1}]$ での分解，および [8] 等にある Nagell, Cassels, Ljunggren, Hemer らの miscellaneous な結果を用いて示される。

$p=5$ としては特に，$N=5\cdot 2^\lambda$, $C_{Q,2}\neq 0$ となる楕円曲線は

$2 \leq \lambda \leq 7$ で互いに non-isomorphic なもの 56 種計算された。実際には $N = 5 \cdot 2^{\lambda}$ の曲線はこれで尽きるものと思われる。

4. conductor と保型関数の理論を結ぶものとして，$\mathbb{Q}$ 上の楕円曲線はすべて Shimura curve の Jacobi 多様体であるという Weil の予想 [19] [3] がある。詳しくかくと C の Zeta 関数（の主要部）を $L(s) = \sum a_n n^{-s}$ とかくと $f(z) = \sum a_n e^{2\pi i n z}$ は $\Gamma_0(N)$ の weight 1 の cusp form になり，C は $\Gamma_0(N)$ に対応する Jacobi 多様体の単純成分に isogenous になるというのである。ここで N はもちろん C の conductor である。だから特に g をこの Jacobian J_N の genus とする場合，

1) $g=0$ となる $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25$ をもつ曲線は存在しない。

2) $g=1$ となる $N = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49$ をもつ曲線は J_N に isogenous になる

が予想される。1) 2) の多くの N について 1), 2) は check されているが一般にはほとんど何も知られていないが $N = 2^{\lambda}$ については Miyawaki の結果がある [7]。われわれの立場で計算した曲線が Fricke [2] の曲線に実際 isomorphic になることを見ることはこの check の一例である。$N = 24, 32, 36$ は Ogg も注意しており，3 で得られる $N = 20$ の曲線の 1 つである

$y^2+x^3+2x^2+5x=0$, 1で注意したように $y^2=x^3+k$ から得られる $N=27$ の $y^2+y+x^3=0$ などでは事実そうなっている。

定理2における order 2 以外の有理点をもつ場合の考察も([10]などを用いて)可能であるし, $N=2^m p^n q^l$ $(p\neq q)$ に対しても同様な結果が得られるであろう。また素数巾 conductor で order 2 以外の order 有限な有理点をもつ曲線は Miyawaki [7] により全て決定されているが有限 order の点を持たない時の決定はずいぶん困難であろうと思われる。そして1でみたように $p\neq 2,3$ に対しては N の p-exponent は2以下であったが $p=2,3$ に対してその上限をもめることは興味ある問題でもあるがそれぞれ, その上限は5および8程度だと予想される。或いは Stufe の N についてよく知られた結果(志村理論などにより) が conductor としての N で云えればそれは Weil 予想の support に他ならないであろう。

文　献

[1]† Baker, A. Effective methods in diophantine problems
Proc. Sympos. Pure Math. 20 (1970) 195–205

[2] Fricke, R. Die Elliptischen Funktionen und ihre Anwendungen
II, (1922)

[3] 本田平．形式群とゼーター関数，第14回代数シンポジウム報告集 (1968)

[4]† Hadano, T. Remarks on the conductor of an elliptic curve, Proc. Japan Acad. 48 (1972) 166–169

[5] 久綱正和，ある型の実2次体の基本単数について(名大 1972)

[6] Ligozat, G. Fonction L des courbes modulaires, Semin. Delange-Pisot-Poitou, 1969/70

[7] 宮脇伸佐夫．[1]楕円曲線のゼータ関数に関するWeil予想について，[2]有限位数有理点をもつ楕円曲線，(共に阪大 1972)

[8] Mordell, L.J. Diophantine Equations. Academic Press (1969)

[9]† Nagell, T. Sur l'impossibilité de quelques équations à deux indéterminés. Norsk Mat For Skrifter, 1 série, 13 (1923)

[10] ——— Sur les propriétés arithmétiques des cubiques planes du premier genre, Acta Math. 52 (1929) 93–126

[11] Néron, A. Modèles minimaux des variétés abeliennes sur les corps locaux et globaux. IHES 21 (1964)

[12] Neumann, O. Die Elliptischen Kurven mit den Führern 3.2^m und 9.2^m, Math. Nachr. 48 (1971) 387–389

[13]† ———, Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. I, Math. Nachr. 49 (1971) 107–123

[14] Ogg, A.P. Abelian curves of 2-power conductor, Proc. Camb. Phil. Soc. 62 (1966) 143–148

[15] ——— Abelian curves of small conductor, J. reine und angew. Math. 226 (1967) 205–215

[16] ——— Elliptic curves and wild ramification, Amer. J. Math. 89 (1967) 1–21

[17] Serre, J.P. and Tate, J. Good reduction of abelian varieties, Ann. of Math. 88 (1968) 492–517

[18]† Vélu, J. Courbes elliptiques sur Q ayant bonne réduction en dehors de {11}. C.R. Acad. Sc. Paris 273 (1971) 73–75

[19] Weil, A. Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Ann. 168 (1967) 149–156

(注) † 印は本文で引用されなかったが，本文に関係があると思われるため便宜上，掲げた文献を意味する．