数理解析研究所講究録
775巻 1992年 93-100

Supersingular j-polynomial と超幾何級数

京都工芸繊維大学工芸学部
金子 昌信
KANEKO Masanobu

序. 標数 p (素数) の体上定義された楕円曲線は原点以外に位数 p の点をもつかもたないかに従って ordinary, supersingular と呼ばれる。p を固定したとき supersingular (以後略して s.s.) な楕円曲線は閉体上の同型を除いて有限個しかない。そこで, それらの有限個の楕円曲線の j-不変量 (閉体上の同型類をパラメトライズする量) を根にもつ多項式を作る:

$$A_p(j) \overset{\text{def}}{=} \prod_{E:\text{s.s.}} (j - j(E))$$

ただし E は標数 p の s.s. 楕円曲線の閉体上の同型類の代表を動き, $j(E)$ をその j-不変量, j は多項式の変数とする.

この $A_p(j)$ は $\mathbb{F}_p[j]$ ($\mathbb{F}_p$ は標数 p の素体) に属しその次数 (即ち s.s. ell. curv. の個数) は $\left[\frac{p+1}{12}\right]+1$ ($p \not\equiv 1 \ (12)$), $\left[\frac{p+1}{12}\right]$ ($p \equiv 1 \ (12)$) (特に ≥ 1), また $\mathbb{F}_p$ 上既約分解したときの既約因子は高々2次, 等々本質的なことはすべて Deuring (1941) によって知られており (その後の Serre, Deligne らによる"現代的な"解釈については [KM] Ch.12 参照), また

これがいわゆる g_2, g_3 ($y^2=4x^3-g_2x-g_3$) からどのように計算されるかも Hasse (1936), Deuring によってわかっている.

以下では, これらのうえにどれだけ新しいものがつけ加わったことになるのかまだはっきりしないのだが, 昨年九州大の Zagier 教授を通じて聞き知った, Atkin による $A_p(j)$ の別の定義法, あるいは計算法というべきか, について述べ, それと超幾何級数との一寸奇妙な結び付きに気付いたのでそれを報告したい。

Atkin の定理

整係数巾級数環 $\mathbb{Z}[[q]]$ の中の元 E_2 を

$$E_2 := 1-24\sum_{n=1}^{\infty}\sigma_1(n)q^n \quad (\sigma_1(n)=\sum_{d|n}d)$$

で定義する。これは $SL_2(\mathbb{Z})$ に関する重さ 2 の Eisenstein 級数の Fourier 展開級数である. ($q=e^{2\pi i\tau}$, $(\mathrm{Im}\,\tau>0)$

$E_2=E_2(\tau)$ とするとき $\begin{pmatrix}a&c\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})$ に対し

$$E_2\left(\frac{a\tau+c}{c\tau+d}\right)=(c\tau+d)^2E_2(\tau)+12\cdot\frac{c(c\tau+d)}{2\pi i}.$$

($E_2=d\log\Delta$ (Δ は重さ 12 の cusp form) である)

さて有理数体上の多項式環 $\mathbb{Q}[j]$ に内積 $(\ ,\ )$ を

$$(f,g):=\mathrm{Res}_{q=0}\,f(j(q))g(j(q))E_2\frac{dq}{q}$$

で入れる. ただし $f(j(q))$, $g(j(q))$ はそれぞれ $f,g\in\mathbb{Q}[j]$ に $j=\frac{1}{q}+744+196884q+\cdots$ (j-不変量の Fourier 展開級数)

を代入してえられる $\mathbb{Q}((q))$ の元（Laurent級数）.

$\mathrm{Res}_{q=0}(\ *\ )\frac{dq}{q}$ はつまり（＊）の定数項である.

これは $(f,f)=0 \Rightarrow f=0$ をみたし，従ってモニック多項式の直交系 $\{P_n(j)\}_{n\geq 0}$ が一意に定まる。即ち $P_n(j)$ はモニック，n 次で $m\neq n \Rightarrow (P_m,P_n)=0$.

例. $P_0(j)=1$.

$P_1(j)=j+a$ とおくと

$$0=(1,P_1)=\mathrm{Res}_{q=0}\left(\frac{1}{q}+744+a+\cdots\right)(1-24q+\cdots)\frac{dq}{q}$$

$$=744+a-24 \quad ;\ a=-720.$$

$P_1(j)=j-720$.

$P_2(j)$ は $(P_0,P_2)=(P_1,P_2)=0$ から定まって.

$P_2(j)=j^2-1640j+269280$. 等.

Theorem（Atkin, 1980ごろ？，多分未発表）

p を素数，$n=n_p$ を標数 p の S.S. j-invariant の個数（$\fallingdotseq \frac{p}{12}$）とする．このとき $P_n(j)$ の係数は p-integral で，

$A_p(j) = P_n(j) \bmod p$ となる.

例. $n_p=1$ となる p は 2, 3, 5, 7, 13 の5つ.

$A_2(j)=A_3(j)=A_5(j)=j$.（考えている環が違うが）

$A_7(j)=j-6$, $A_{13}(j)=j-5$.（例えば [D] の表）

これらはすべて1つの $j-720$ をそれぞれの p で reduction して得られる.

$A_{11}(j) = j(j-1) = P_2(j) \bmod 11$,

$A_{17}(j) = j(j-8) = P_2(j) \bmod 17$ 等.

Atkin のもとの証明は ${}_7F_6$ という超幾何関数の等式を用いた複雑なものであったらしい(小池先生からのまた聞き).

Zagier は "$A_p(j) = E_{p-1} \bmod p$" (Deligne ?) を用いた簡明な証明を与えた. ここでは証明は省かせていただく。この Zagier の証明に inspire されて次のようなことを考えた.

Gauss 超幾何級数との関係

$$F(\alpha,\beta,\gamma,x) = 1 + \frac{\alpha\cdot\beta}{1\cdot\gamma}x + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot 2\cdot\gamma(\gamma+1)}x^2 + \cdots$$

を Gauss の超幾何級数とし次の連分数展開を考える

$$\frac{F(\frac{5}{12},\frac{13}{12},1,12^3x)}{F(\frac{5}{12},\frac{1}{12},1,12^3x)} = \cfrac{1}{1-\cfrac{a_1x}{1-\cfrac{a_2x}{1-\cfrac{a_3x}{1-\cdots}}}}$$

このような2つの超幾何の比の連分数展開は Gauss [G] によって一般的に与えられてあって, 今の場合 a_i は

$a_1 = 720$, $a_{2n} = 12\cdot\frac{(12n-5)(12n+1)}{(2n-1)\cdot 2n}$, $a_{2n+1} = 12\cdot\frac{(12n-1)(12n+5)}{2n(2n+1)}$ $(n\geq 1)$
と計算エルる.

さてこの連分数の第 $2n-1$ convergent を $f_n(x)$ とする:

$$f_n(x) = \cfrac{1}{1-\cfrac{a_1 x}{1-\cfrac{a_2 x}{\ddots\ \cfrac{1}{1-a_{2n-1}x}}}}.$$

これを $f_n(x) = \frac{h_n(x)}{g_n(x)}$, $g_n(0) = h_n(0) = 1$. $\deg g_n = n$, $\deg h_n = n-1$ と書く. このとき.

Theorem $\quad P_n(j) = j^n g_n\left(\frac{1}{j}\right)$

つまり先程の直交系 $\{P_n(j)\}$ は, 上の超幾何級数の比の連分数展開を途中で切ってえられる"近似分数"の分母の系列としても得られる.

この定理は、連分数展開が等式

$$-\frac{j}{q\frac{dj}{dq}}\cdot E_2 = \frac{F\left(\frac{5}{12},\frac{13}{12},1,\frac{12^3}{j}\right)}{F\left(\frac{5}{12},\frac{1}{12},1,\frac{12^3}{j}\right)} \quad (\text{in } \mathbb{Q}((q)))$$

によって Atkin の内積に直接結びついており. 依って単なる再解釈であるといえる. しかしこのように見ることで例えば漸化式:

Cor. $P_{n+1}(j) = \{j - (a_{2n} + a_{2n+1})\} P_n(j) - a_{2n-1} \cdot a_{2n} P_{n-1}(j)$.

$n \geq 1$, $P_0 = 1$, $P_1 = j - 720$

などが明解に証明される. (この漸化式は $A_p(j)$ の実際の計算に極めて有効)

Supersingular λ-polynomial

同様のことは s.s. λ-invariant ($\leftrightarrow y^2 = x(x-1)(x-\lambda)$) についても行うことができる. 詳しい説明は略して結果だけ書くと次のようになる.

$$E_2^* := 1 - 8 \sum_{n=1}^{\infty} \Big(\sum_{\substack{d \mid n \\ n/d \equiv 0 (2)}} (-1)^d d \Big) q^n$$

$$= 1 - 8 \sum_{n=1}^{\infty} (\sigma_1(n) - 2\sigma_1^{odd}(n)) q^{2n}$$

$$\Big(\sigma_1(n) = \sum_{d \mid n} d \ , \ \sigma_1^{odd}(n) = \sum_{\substack{d \mid n \\ odd}} d \Big) ,$$

$$\lambda(q) := \left(\frac{1 + 2\sum_{n=1}^{\infty} q^{n^2}}{q \sum_{n=0}^{\infty} q^{n(n+1)}} \right)^4 = \frac{1}{q} + 8 + 20q - 62q^3 + \cdots$$

$(q = e^{\pi i \tau})$

とおく. (ふつう "λ" は $16/\lambda(q)$ をとるようである)

$\mathbb{Q}[\lambda]$ の内積を

$$(f, g) = \mathrm{Res}_{q=0} f(\lambda(q)) g(\lambda(q)) E_2^* \frac{dq}{q}$$

で入れ, モニック直交系を $\{L_n(\lambda)\}_{n \geq 0}$ とする.

このとき，3以上の素数 p に対し，$L_{\frac{p-1}{2}}(\lambda) \bmod p$ が
"supersingular λ-polynomial" を与える．
古典的な $\sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \lambda^i \bmod p$ は $\left(\frac{\lambda}{16}\right)^{\frac{p-1}{2}} L_{\frac{p-1}{2}}\left(\frac{16}{\lambda}\right) \bmod p$
に等しい．

算式 $$-\lambda \frac{E_2^*}{q\frac{d\lambda}{dq}} = \frac{F\left(\frac{1}{2}, \frac{3}{2}, 1, 16/\lambda\right)}{F\left(\frac{1}{2}, \frac{1}{2}, 1, 16/\lambda\right)}$$ より

右辺の連分数展開の"近似分母"としても $L_n(\lambda)$ は得られる．

漸化式 $L_{n+1}(\lambda) = (\lambda - 8)L_n(\lambda) - 4\frac{(2n-3)(2n+1)}{n(n-1)}L_{n-1}(\lambda)$，$n \geq 2$

$$L_1 = \lambda - 8,\ L_2 = \lambda^2 - 16\lambda + 16$$

は $y^2 = x(x-1)(x-\lambda)$ の $\mathbb{F}_p$-有理点の個数の計算に役立つかもしれないが，あまり考えてみていないので何とも言えない．

終わりに

以上述べたことは正直なところまだよく意味がわからない．しかし面白い．Elkiesの言葉を借りると「It's cute, even if as of now it's only a curiosity.」何かすっきりした解釈がつかないかと思っている．

文献

[D] M. Deuring ; Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamburg, 14 (1941), 197-272

[G] C.F. Gauss ; Disquisitiones generales circa seriem infinitam $1+\frac{\alpha\beta}{1\cdot\gamma}x+\frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot2\cdot\gamma(\gamma+1)}xx+\frac{\alpha(\alpha+1)(\alpha+2)\beta(\beta+1)(\beta+2)}{1\cdot2\cdot3\cdot\gamma(\gamma+1)(\gamma+2)}x^3+\text{etc.}$ 1812, 全集 vol. III. 125-162.

[H] H. Hasse ; Zur Theorie der abstrakten Funktionenkörper, I. Journ. f. d. r. u. ang. Math. 175, (1936) 55-62.

[KM] N. Katz - B. Mazur ; Arithmetic moduli of elliptic curves. Annals of Math. Studies, 1985, Princeton

付 [D] の表 (p. 257-258) に誤植がある.

$p=73$ に対する $P_p(j)$ は (我々の $A_p(j)$)

$$j^6+60j^5+68j^4+9j^3+38j^2+39j+7$$

$p=97$ に対する $P_p(j)$ は

$$j^8+60j^7+10j^6+96j^5+2j^4+72j^3+3j^2+28j+19$$

が正しい. ただし, どちらも $P_p(j)$ の根として書いてあるリストは正しい.