

超特異楕円曲線と超幾何級数(代数的数論 : 最近の 進展とその背景)

金子, 昌信
京都工芸繊維大学工芸学部

<https://hdl.handle.net/2324/4755269>

出版情報 : 京都大学数理解析研究所講究録. 844, pp.17-25, 1993-06. Research Institute for
Mathematical Sciences (RIMS), Kyoto University

バージョン :

権利関係 :



超特異楕円曲線と超幾何級数

京都工繊大 工学部

金子 昌信

Kaneko Masanobu

表記のタイトルですぐ頭に浮かぶのは、有限体上の楕円曲線を Legendre の標準形 $y^2 = x(x-1)(x-\lambda)$ で書いたときこのいわゆる Hasse invariant が本質的に Gauss の超幾何級数 $F(\frac{1}{2}, \frac{1}{2}, 1, \lambda)$ で与えられるという古典的な事実 (Deuring [3], Igusa [5]) であらうかと思います。

(この研究会に先立って行われた「Automorphic forms and L-functions」の報告集の中で小池先生がこのことを有限体上の超幾何曲線の立場から書かれています。) Deuring は Weierstrass の標準形の時も Hasse invariant を j -invariant で具体的に計算しており、それが超幾何級数であるということは更にいくつかの変形を要するのですがとにかく O.K. で、これも「知っている人は知っている」ことかと思います。(Atkin [1], Namba [8])

さて Hasse invariant ということは結局次の対象を相手にすることになります。

$$SS_p(j) := \prod_{E: S.S} (j - j(E))$$

ここに E は標数 p の supersingular 楕円曲線の肉体上の同型類の代表をとり, $j(E)$ をその j -不変量とします。

これは各素数 p を与えるごとに Deuring のようにして具体的に計算できるものですが, Atkin [2] が次のような $\mathbb{Q}$ 上の多項式系 $\{P_n(j)\}_{n \geq 0}$ を構成した。即ち, 各 $P_n(j)$ は n 次モノミュー多項式で, 多項式環 $\mathbb{Q}[j]$ 上のある内積に関して $P_{n_1}(j)$ と $P_{n_2}(j)$ ($n_1 \neq n_2$) は直交しており, 素数 p に対して $n = \deg SS_p(j)$ とするとき $P_n(j) \bmod p = SS_p(j)$ 。はじめのいくつかを書き出すと。

$$P_0(j) = 1,$$

$$P_1(j) = j - 720,$$

$$P_2(j) = j^2 - 1640j + 269280,$$

$$P_3(j) = j^3 - \frac{12576}{5}j^2 + 1526958j - 107765856,$$

$$P_4(j) = j^4 - 3384j^3 + 3528552j^2 - 1133263680j + 44184000960.$$

例えば $p = 2, 3, 5, 7, 13$ に対して $\deg SS_p(j) = 1$ となりますから (一般に $\deg SS_p(j) = \frac{1}{12}(p-1) + \frac{1}{3}(1 - (\frac{-3}{p})) + \frac{1}{4}(1 - (\frac{-4}{p}))$) これらの p で $P_1(j) = j - 720$ を $\bmod p$ すれば $SS_p(j)$ を得, $p = 11, 17, 19$ に対しては $P_2(j)$, という具合です。

この $P_n(j)$ を定める内積の定義は以前 [6] に書きました。(整数論の人の目には殆んど触れなかったのではないかと思います) そこで $P_n(j)$ の別の構成法, つまり Gauss の超幾何級数のある比を連分数展開してその近似分数の分母としてえられる多項式の系列が即ち $P_n(j)$ であることを報告したのでありますが, その証明は Hasse invariant = Eisenstein series mod p という事実を使った Zagier 氏による Atkin の定理 ($SS_p(j) = P_n(j) \bmod p$) の証明に依存しており, $SS_p(j)$ と超幾何の結びつきということをはっきり見えてきませんでした。

今回の講演で話しましたことは, Deuring の計算をさらに進めてえられる $SS_p(j)$, 或いはもう少し精密に Frobenius trace mod p の超幾何級数による具体的な表示, Atkin の内積の定義と [6] で述べに連分数との関係 (別のタイプの連分数を使って述べましたが), 及びそれからえられる corollary でした。はじめの $SS_p(j)$ の表示を使うと Atkin の多項式 $P_n(j)$ と超幾何からくる連分数の結びつきがよくわかり, すべて初等的に理解できるようになった, というのが話のポイントであったつもりなのですが, 連分数との関係は証明を書くか否ければ statement は [6] に書きましたのでここでは省くこととし, Frobenius trace の計算結果と (explicit に書いてあるのを余り見ないで書いておくのも無意味では

はいと思います), 最近得られた, $P_n(j)$ の explicit な表示式を書きます。

$y^2 = x^3 + ax + b$ / $\mathbb{F}_p$ の有理点の個数は $p+1-t$ という形に書くと $|t| < 2\sqrt{p}$ で (Hasse) 従って $p \geq 17$ であれば t は $t \bmod p$ で一意的に定まる。 $t \bmod p$ を計算することは結局 $(x^3 + ax + b)^{\frac{p-1}{2}}$ の x^{p-1} の係数 $\bmod p$ を計算することとなり, これをとにかく素朴に計算していくと次がえられる. ただし $j = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2}$

Prop. 1) $j \neq 0$ のとき

$$t \bmod p = \begin{cases} a^{\frac{p-1}{4}} \left(\frac{\frac{p-1}{2}}{\frac{p-1}{4}} \right) F^{(p)} \left(\frac{1}{12}, \frac{5}{12}, \frac{1}{2}, 1 - \frac{1728}{j} \right) & p \equiv 1 (4) \\ a^{\frac{p-1}{4}} b \frac{(\frac{p-1}{2})!}{(\frac{p+1}{4})! (\frac{p-7}{4})!} F^{(p)} \left(\frac{7}{12}, \frac{11}{12}, \frac{3}{2}, 1 - \frac{1728}{j} \right) & p \equiv 3 (4) \end{cases}$$

2) $j \neq 1728$ のとき

$$t \bmod p = \begin{cases} b^{\frac{p-1}{6}} \left(\frac{\frac{p-1}{2}}{\frac{p-1}{3}} \right) F^{(p)} \left(\frac{1}{12}, \frac{7}{12}, \frac{2}{3}, \frac{j}{j-1728} \right) & p \equiv 1 (3) \\ a b^{\frac{p-5}{6}} \frac{(\frac{p-1}{2})!}{(\frac{p-5}{6})! (\frac{p-2}{3})!} F^{(p)} \left(\frac{5}{12}, \frac{11}{12}, \frac{4}{3}, \frac{j}{j-1728} \right) & p \equiv 2 (3) \end{cases}$$

ここで $F^{(p)}(\frac{1}{12}, \frac{5}{12}, \frac{1}{2}, x)$ 等は Gauss の超幾何級数を $[\frac{p}{12}]$ 次のところで打ち切り、えられる多項式を $\text{mod } p$ (にもの). 或いは $F^{(p)}(\frac{1}{12}, \frac{5}{12}, \frac{1}{2}, x) = F(\frac{1}{12}, \frac{5}{12}, \frac{1}{2}, x)^{1-p} \text{ mod } p$ 等.

今, $F(\frac{1}{12}, \frac{5}{12}, \frac{1}{2}, 1-x)$ (resp. $F(\frac{7}{12}, \frac{11}{12}, \frac{3}{2}, 1-x)$) と $F(\frac{1}{12}, \frac{5}{12}, 1, x)$ (resp. $F(\frac{7}{12}, \frac{11}{12}, 1, x)$) が同じ微分方程式を満たすことと $F(\frac{1}{12}, \frac{5}{12}, \frac{1}{2}, x)$ 等の $\frac{p}{12} \sim p-1$ 次の係数が $\text{mod } p$ で 0 ということから, $F^{(p)}(\frac{1}{12}, \frac{5}{12}, \frac{1}{2}, 1-x)$ (resp. $F^{(p)}(\frac{7}{12}, \frac{11}{12}, \frac{3}{2}, 1-x)$) と $F^{(p)}(\frac{1}{12}, \frac{5}{12}, 1, x)$ (resp. $F^{(p)}(\frac{7}{12}, \frac{11}{12}, 1, x)$) は定数倍しか違わないことがわかる. 最高次の係数を比べることにより, 例えば $j \neq 0$ のとき, 次の $\text{mod } p$ は次のようにも書ける.

Prop. $j \neq 0$ とする. $S_n = (-1)^n \cdot 2^{-2n} \binom{2n}{n}$ と書く.

$$t \text{ mod } p = \begin{cases} \frac{S_{\frac{p-1}{4}}}{S_{\frac{p-1}{12}}} \times a^{\frac{p-1}{4}} F^{(p)}(\frac{1}{12}, \frac{5}{12}, 1, \frac{1728}{j}) & p \equiv 1 \pmod{12} \\ \frac{S_{\frac{p-1}{4}}}{S_{\frac{p-5}{12}}} \times a^{\frac{p-1}{4}} F^{(p)}(\frac{1}{12}, \frac{5}{12}, 1, \frac{1728}{j}) & p \equiv 5 \pmod{12} \\ \frac{9}{2} \times \frac{S_{\frac{p-3}{4}}}{S_{\frac{p-7}{12}}} \times a^{\frac{p-7}{4}} \cdot b \cdot F^{(p)}(\frac{7}{12}, \frac{11}{12}, 1, \frac{1728}{j}) & p \equiv 7 \pmod{12} \\ \frac{9}{10} \times \frac{S_{\frac{p-3}{4}}}{S_{\frac{p-11}{12}}} \times a^{\frac{p-7}{4}} \cdot b \cdot F^{(p)}(\frac{7}{12}, \frac{11}{12}, 1, \frac{1728}{j}) & p \equiv 11 \pmod{12} \end{cases}$$

(右辺全て $\text{mod } p$)

$p \equiv 1 (4)$ のときは $S_{\frac{p-1}{4}}/S_{\frac{p-1}{12}}, S_{\frac{p-1}{4}}/S_{\frac{p-5}{12}} \pmod p$ は
 実際には ± 1 , 1 の 4 乗根, である。且つ $\frac{p-1}{12}$ は

$$S_{\frac{p-1}{4}}/S_{\frac{p-1}{12}} \equiv \left(\frac{(\frac{p-1}{3})!}{p} \right) \pmod p$$

$$S_{\frac{p-1}{4}}/S_{\frac{p-5}{12}} \equiv \left(\frac{(\frac{p-2}{3})!}{p} \right) \left(\frac{p-1}{2} \right)! \pmod p \quad \text{と予想される}$$

が, 証明できていない。

この計算 (と同じことを $\overline{\mathbb{F}_p}$ 上でやっても可) から系として
 $SS_p(j)$ は次のようになる。

$$\text{系} \quad SS_p(j) = \begin{cases} j^{\frac{p-1}{12}} F^{(p)}\left(\frac{1}{12}, \frac{5}{12}, 1, \frac{1728}{j}\right) & p \equiv 1 (12) \\ j^{\frac{p+7}{12}} F^{(p)}\left(\frac{1}{12}, \frac{5}{12}, 1, \frac{1728}{j}\right) & p \equiv 5 (12) \\ j^{\frac{p-7}{12}} (j-1728) F^{(p)}\left(\frac{7}{12}, \frac{11}{12}, 1, \frac{1728}{j}\right) & p \equiv 7 (12) \\ j^{\frac{p+1}{12}} (j-1728) F^{(p)}\left(\frac{7}{12}, \frac{11}{12}, 1, \frac{1728}{j}\right) & p \equiv 11 (12) \end{cases}$$

これから, Atkin の多項式を [6] のように $\frac{F(\frac{13}{12}, \frac{5}{12}, 1, x)}{F(\frac{1}{12}, \frac{5}{12}, 1, x)}$
 の連分教展開から再構成できる。

ところで、超幾何級数の比 $F(\alpha+1, \beta, \gamma, x) / F(\alpha, \beta, \gamma, x)$ を

$$\frac{F(\alpha+1, \beta, \gamma, x)}{F(\alpha, \beta, \gamma, x)} = \frac{1}{1 - \frac{a_1 x}{1 - \frac{a_2 x}{1 - \frac{a_3 x}{\ddots}}}}$$

と連分数展開 (a_i は Gauss [4] による, $a_1 = \frac{\beta}{\gamma}$, $a_{2n} = \frac{(\alpha+n)(\gamma-\beta+n-1)}{(\gamma+2n-2)(\gamma+2n-1)}$, $a_{2n+1} = \frac{(\beta+n)(\gamma-\alpha+n-1)}{(\gamma+2n-1)(\gamma+2n)}$ ($n \geq 1$)), $a_{n+1} = 0$ とおいてえられる第 n 近似有理式 (n -th convergent) を $T_n(x) / S_n(x)$ とすると ($S_n(0) = T_n(0) = 1$),

Theorem

$$S_n(x) = \sum_{i=0}^{\lfloor \frac{n+1}{2} \rfloor} \sum_{k=0}^i (-1)^i \binom{-\alpha}{k} \binom{-\beta}{k} \binom{-\gamma}{k} \binom{\alpha + \lfloor \frac{n+1}{2} \rfloor}{i-k} \binom{\beta + \lfloor \frac{n}{2} \rfloor}{i-k} \binom{\gamma+n-1}{i-k} x^i$$

$$\left(= \sum_{i=0}^{\lfloor \frac{n+1}{2} \rfloor} \sum_{k=0}^i \frac{(\alpha)_k (\beta)_k}{k! (\gamma)_k} \cdot \frac{(-\alpha - \lfloor \frac{n+1}{2} \rfloor)_{i-k} (-\beta - \lfloor \frac{n}{2} \rfloor)_{i-k}}{(i-k)! (-\gamma - n + 1)_{i-k}} \cdot x^i \right)$$

$$T_n(x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \sum_{k=0}^i (-1)^i \binom{\alpha-1}{k} \binom{-\beta}{k} \binom{-\gamma}{k} \binom{\alpha + \lfloor \frac{n+1}{2} \rfloor}{i-k} \binom{\beta + \lfloor \frac{n}{2} \rfloor}{i-k} \binom{\gamma+n-1}{i-k} x^i$$

$\alpha = \frac{1}{12}, \beta = \frac{5}{12}, \gamma = 1$ としにときの $j^n S_{2n-1}(\frac{1}{j})$
 が $P_n(j)$ であるから.

$$\text{系} \quad P_n(j) = \sum_{i=0}^n \sum_{k=0}^i (-1)^{i-k} \binom{-\frac{1}{12}}{k} \binom{-\frac{5}{12}}{k} \binom{\frac{1}{12}+n}{i-k} \binom{\frac{5}{12}+n-1}{i-k} \frac{j^{n-i}}{\binom{2n-1}{i-k}}$$

これがどう使えるかはこれからのものであるが.

[6] で書いた Atkin の内積の定義は他にもいくつか同値
 はないかえがあり, さらにこれは, $j = j(\tau)$ (elliptic
 modular function) とみなときの Hecke 作用素の作用に
 ついて Hermitian ということで定数倍を除いて特徴付けられ
 るようで, そうなると非常に canonical なものというこ
 にはなります. こういったことや, 今まで書いてきた諸々の
 ことは Zagier 氏と共著の論文を準備中 ([7]) ですの
 で, そこで詳しく書くつもりです.

文献

- [1] A.O.L. Atkin ; Modular forms of weight one,
 and supersingular equations, (? 日本数学, シン
 197?, 済みせん. 時間の関係で済みせんといふ.)

- [2] A.O.L. Atkin; Talk, MPI, Bonn, 1985, 6, 20.
- [3] M. Deuring; Die Typen der Multiplikatorringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamburg, 14 (1941), 197-272.
- [4] C.F. Gauss; Disquisitiones generales circa seriem infinitam $1 + \frac{\alpha\beta}{1\cdot r}x + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot 2\cdot r(r+1)}x^2 + \frac{\alpha(\alpha+1)(\alpha+2)\beta(\beta+1)(\beta+2)}{1\cdot 2\cdot 3\cdot r(r+1)(r+2)}x^3 + \text{etc.}$
1812, 全集 vol III, 125-162.
- [5] J-I. Igusa; Class number of a definite quaternion with prime discriminant, Proc. N.A.S. 44 (1958), 312-314.
- [6] M. Kaneko; Supersingular j -polynomial と超幾何級数, 数理解析講究録 775, Einstein 計量と Yang-Mills 接続, 1992年3月, 93-100
- [7] M. Kaneko - D. Zagier; Supersingular j -invariants, hypergeometric series, and Atkin's orthogonal polynomials, in preparation
- [8] K. Namba; Hessian family $x^3 + y^3 + z^3 = 3\alpha xyz$, $F(\frac{1}{3}, \frac{2}{3}, 1, z)$ and $p = 3n^2 + 3n + 1$, 日本数学会 1992年度秋季総合分科会 数学基礎論分科会 講演アブストラクト, 1992年10月, 名古屋大学, 21-22.

(雑な報告にしてみました。おわびします)