楕円曲線の j 不変量に関する話題*

九州大学　数理学研究科　金子昌信

はじめに個人的なことを少し。自分がはじめて j invariant というものに出会ったのがいつだったか、もう正確には思い出せませんが、 “official” には、学部 4 年のゼミで伊原康隆先生のもと、Lang の “Elliptic Functions” を読んだとき、となるかもしれません。その時、参考文献に挙げてあった Fricke や Weber の本に少し分け入って以来、j 関数というのは数学の中で最もお気に入りの対象となりました。そのあと 院生 のとき近藤武先生の Moonshine の講義を聞いたりしてますます愛着を深めていきましたが、その頃は自分で何か “j” について仕事が出来るとは想像もしていませんでした。ところが博士課程も終りという頃に Noam Elkies の論文が出て、これが非常に自分の好みに合って、幸いそこから一つ仕事が出来ました。それが阪大に助手にとっていただいて最初の年で、山本芳彦先生に初めて数式処理なるものの存在を知らされ、手ほどきを受けられたことも大きな力となりました。その後 Don Zagier さんに出会ったりして、本当に幸運なことに、いくつか j に関する仕事が出来ました。自分としては望外の喜びで、j についての報告を書くこの機会に上に述べた方々に心から感謝を表したいと思います。

以下の小文ではその “j” について、主に自分が関わってきたことを中心に述べます。歴史についてももっと調べて書けるとよかったのですが、力及びませんでした。他日を期したい（できれば）と思います。

1　楕円モジュラー関数 $j(\tau)$

はじめに複素数体上の場合、即ち古典的な楕円モジュラー関数 $j(\tau)$ についていくつかのトピックをのべ、次章で有限体上の場合の話、特に supersingular j invariant について述べる。最後の第 3 章は最近の超越数論における $j(\tau)$ に関連した話題の簡単な紹介である。末尾に文献を少し詳しくつけたので、興味を持たれたトピックがあれば原論文にあたっていただきたいと思う。

1.1　定義

複素平面 $\mathbf{C}$ 内の格子 $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ をとり、L を周期とする Weierstrass の楕円関数

$$\wp(z) = \wp(z; L) := \frac{1}{z^2} + \sum_{\omega \in L\setminus\{0\}} \left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\}$$

を考える。この $\wp(z)$ は微分方程式

$$\wp\prime(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L), \quad \left(g_2(L) = 60 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^4}, \;\; g_3(L) = 140 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^6} \right)$$

を満たし、これを通して Riemann 面としての複素トーラス $\mathbf{C}/L$ と複素数体上の楕円曲線

$$Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3 \quad (g_2 = g_2(L), g_3 = g_3(L))$$

* 代数学シンポジウム（1996 年 7 月　山形）講演報告集原稿

とが同一視されるのであった。複素数体上の楕円曲線を上の形にかいたとき、その j 不変量とは係数から代数的に

$$j := 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$$

で与えられる量のことであり、それによって曲線の同型類が複素数によってパラメトライズされる。つまり複素数体上の楕円曲線の同型類全体の集合は j 不変量により複素数全体と同一視される。この j 不変量を上の対応を通して格子の (ω_1, ω_2 の) 関数と思うと、その値は比 $\tau := \omega_2/\omega_1$ (常に $Im(\tau) > 0$ となるようにとる) のみによる。こうして得られる複素上半平面 $\mathbf{H} := \{\tau \in \mathbf{C} | Im(\tau) > 0\}$ 上の正則関数がすなわち楕円モジュラー関数 $j(\tau)$ である：

$$j(\tau) = 1728\frac{\left(60\sum_{\substack{m,n\in\mathbf{Z}\\(m,n)\neq(0,0)}}\frac{1}{(m\tau+n)^4}\right)^3}{\left(60\sum_{\substack{m,n\in\mathbf{Z}\\(m,n)\neq(0,0)}}\frac{1}{(m\tau+n)^4}\right)^3 - 27\left(140\sum_{\substack{m,n\in\mathbf{Z}\\(m,n)\neq(0,0)}}\frac{1}{(m\tau+n)^6}\right)^2}.$$

先の対応でトーラスとしての同型（格子が定数倍で移りあう）と楕円曲線としての同型が同じことになるので、$j(\tau)$ は複素トーラスの同型類をパラメトライズするということになり、それは

1) $j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau)$ が $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ に対して成り立ち、

2) $j(\tau) = j(\tau')$ ならばある $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ があって $\tau' = \frac{a\tau+b}{c\tau+d}$ となる、

ということに外ならない。

1.2 Fourier 展開—Monstrous Moonshine

上の性質 1) から特に $j(\tau+1) = j(\tau)$, したがって (正則性と併せて) $j(\tau)$ は $q = e^{2\pi i\tau}$ の Fourier 級数に展開される。その形は、 g_2, g_3 の q 展開の古くから知られる公式により、

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n$$

となり、さらに各 c_n は正整数になることがわかる。($c_0 = 744, c_1 = 196884, c_2 = 21493760, c_3 = 864299970, \ldots$) より正確には、公式

$$j(\tau) = \frac{\left(1 + 240\sum_{d=1}^{\infty}\frac{d^3q^d}{1-q^d}\right)^3}{q\prod_{n=1}^{\infty}(1-q^n)^{24}}$$

からこれらのことがわかる。

解析的な手法を用いてこの c_n の公式を与えたのが H. Petersson (1932) と H. Rademacher (1938) である。二人は独立に全く別の方法で同じ公式を導いた：

$$c_n = \frac{2\pi}{\sqrt{n}} \sum_{k=1}^{\infty} \frac{A_k(n)}{k} I_1\left(\frac{4\pi\sqrt{n}}{k}\right) \quad (n \geq 1)$$

ここに

$$A_k(n) = \sum_{\substack{h \bmod k \\ hh' \equiv -1(k)}} exp\left(-\frac{2\pi i}{k}(nh + h')\right) \quad \text{(Kloosterman sum)}$$

および

$$I_1(x) = \sum_{m=0}^{\infty} \frac{(x/2)^{2m+1}}{m!(m+1)!} \quad \text{(第一種変形 Bessel 関数)}$$

である。この公式から c_n の漸近公式

$$c_n \sim \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}n^{3/4}} \quad (n \to \infty)$$

が得られる。また Rademacher は、逆にこの公式から c_n を定義し、それから Fourier 級数 $\frac{1}{q} + \sum_{n=1}^{\infty} c_n q^n$ を作るとこれが $SL_2(\mathbf{Z})$ で不変となることを示す論文も書いている (1939) 。

また c_n についての仕事には、D.H. Lehmer, J. Lehner, O. Kolberg, A.O.L. Atkin, M. Koike らによる、小さな素数のべきを法とする c_n の満たす合同式の研究や、p 進的な性質の研究がある。この方面もまだ分かってないことが多いようである。そのほかにも色々あることと思うが、やはり $j(\tau)$ の Fourier 係数に関して最も多くの注目を惹いた仕事は J. Conway-S. Norton (1979) による所謂 Monstrous Moonshine であろう。彼等の仕事は $j(\tau)$ にとどまるものではないが、その発端は、$j(\tau)$ の Fourier 係数のはじめのいくつかが、Monster 単純群の既約表現の次数の簡単な和として書けるという J. Mckay や J. Thompson の観察である。Mckay さんは先頃九大のセミナーで話をされたが、話の途中で着ている T シャツを脱いだかと思うと、その下がまた別の T シャツ、くるっと向けたその背には

$$196884$$
$$\|$$
$$1 + 196883$$

とプリントされてあった。余談はさておき、のちに I. Frenkel-J. Lepowsky-A. Meurman は Monster 群が作用する無限次元の次数つきベクトル空間で、その各次数が c_n になっているものを構成することにより $j(\tau)$ に関する “Moonshine ” を証明した。それは Conway-Norton の予想の、 Monster 群の単位元に対応する部分で、別の元に対応する部分は最終的に R. Borcherds (1992) によって証明された。Frenkel-Lepowsky-Meurman や Borcherds の証明で中心的な役割を果たしている数学的対象が vertex operator algebra と呼ばれるものである。これはそもそも物理の string theory から出てきた対象で、私はいまだによく理解していない。しかし物理世界の究極像を数学的に記述しようとする試みの中に ”究極のシンメトリー” Monster 単純群がたち現われ、またさらに最も根本的な保型関数、楕円モジュラー関数 $j(\tau)$ が現われてくるというのは何ともいえず楽しい。” 物理学者が宇宙の構造の中に思いも掛けぬ仕方で組み込まれているモンスター群に偶然出会うであろう ” というのはかつて物理学者 F. Dyson が夢見たことであった。

1.3 Singular moduli (虚数乗法論)

複素数体上の楕円曲線はその準同型環が $\mathbf{Z}$ より大きくなるとき虚数乗法をもつとか CM 型 (CM=complex multiplication) であるとかいう。(このとき準同型環は虚 2 次整環、つまり虚 2 次体の整数環の部分環で $\mathbf{Z}$ 上の rank が 2 のもの、になる。) 虚数乗法を持つとき対応する τ は虚 2 次無理数で、虚数乗法を持つ楕円曲線の j 不変量、すなわち j 関数の虚 2 次数での値を伝統的に singular moduli (singuläre Moduln) (複数形) という。古典的な虚数乗法論はその値の性格を教えるが、それを一番ラフな形で述べると次のようになる。

定理 $\tau_0 \in \mathbf{H}$ を虚 2 次体 k の数とする。このとき、$j(\tau_0)$ は代数的数であり、k にそれを添加した体は k 上のある Abel 拡大となる。

ちなみに、虚 2 次体の虚数乗法論は Kronecker にその大部分を負うのだろうが、現今の本に見られるように j 関数を使って定式化したのは Georg Pick (1885, 1886) が H. Weber に先立つようである。あとで必要な記号を導入するためにも、その j 関数の虚数乗法論をもう少し詳しく復習しておこう。今 $-d$ を虚 2 次整環の判別式、つまり d は正整数で $\equiv 0$ or $3\ mod\ 4$ とする。判別式 $-d$ の整環を O_d と書く。これに対し、proper O_d ideal, つまり、$\mathbf{Q}(\sqrt{-d})$ 内の lattice であってその乗数環 (それをかけてもその lattice からはみ出さない、ような数全体) が丁度 O_d になっているもの、の普通の意味での lattice としての (ideal としての) 同値類を考える。するとこの同値類全体には有限 Abel 群の構造が入ることがわかる。これを proper O_d ideal class group, その位数を O_d の類数と呼びそれぞれ $C\ell(d), h(d)$ で表わす。(本当は d の代わりに $-d$ を入れるべきだが実 2 次体は登場しないので誤解はないと思う。) $C\ell(d)$ の代表元を Λ_1 から Λ_h, $h = h(d)$ とする。さて、このとき上の定理はより詳しく次のように述べられる。

定理 $\tau_0 \in \mathbf{H}$ を虚 2 次体 k の数とし、1 と τ_0 で生成される lattice の乗数環が O_d だとする。このとき、$j(\tau_0)$ は $\mathbf{Q}$ 上 $h(d)$ 次の代数的整数である。さらに $j(\tau_0)$ は k 上のいわゆる環類体という Abel 拡大を生成し、その k 上の Galois 群は $C\ell(d)$ と標準的に同型になる。その同型を通しての $C\ell(d)$ の $j(\tau_0)$ への作用も explicit に書け、$j(\Lambda_i)$, $1 \le i \le h(d)$ が $j(\tau_0)$ の $\mathbf{Q}$ 上の共役を丁度与える。(j 関数は lattice の関数であったことに注意)

k 上の Abel 拡大すべてを得るためにはこれだけでは不十分で、楕円関数の等分値が必要になる。ここではしかしそちらには立ち入らない。巻末の文献参照。

上のことから、判別式 $-d$ を一つ与えると、上の $j(\Lambda_i)$ たちを丁度根に持つような $\mathbf{Z}$ 上の monic 多項式 (変数を j で表わすことにする) が定まる。これを判別式 $-d$ の類多項式 (class polynomial) と呼び、ここでは $P_d(j)$ とかく。$P_d(j)$ の次数は $h(d)$ である。

例： $P_3(j) = j$, $P_4(j) = j - 1728$, $P_7(j) = j + 3375$, $P_8(j) = j - 8000$, $P_{11}(j) = j + 32768$, $P_{12}(j) = j - 54000$, $P_{15}(j) = j^2 + 191025j - 121287375$, ...

1.4 Borcherds の無限積

Borcherds はその最近の仕事において、generalized Kac-Moody algebra の理論に導かれて、ある種の保型形式の無限積公式を与えた。これについては本報告集中の浅井哲也さんの報告を参照していただきたいが、この Borcherds の仕事は（一変数の場合）j 関数の虚数乗法についての新しい視点を提供しているように思われる。Borcherds の定理を一変数に限って極めて大ざっぱに述べるとすると、

定理 (Borcherds, 1995)　類多項式は意味のある無限積表示を持つ。

ということになる。具体的には、$P_d(j)$ の j のところに $j(\tau)$ の q 展開を代入して、形式的に

$$q^{-h}\prod_{n=1}^{\infty}(1-q^n)^{a_n}$$

の形に書いたとき、肩に現われる a_n がある種の半整数 weight の modular form の Fourier 係数になっているというのである。類多項式は上半平面上に零点を持つからこの無限積は local にしか収束しない。上のように言ってしまうと分かりにくいが、論文を読むと Borcherds の定理は一見して Shimura 対応を連想させる。さて、どんな世界がそこから広がって行くのであろうか。より詳しくは浅井さんの論説や原論文を見ていただくとして、ここではこの Borcherds の定理と essential に同値であるところの D. Zagier による次の定理をきちんと述べよう。(essential に同値といっても決して自明な言い替えなどではない。これについてはまだ書かれたものがないが、私の手書きの覚え書き程度でよければ、言って下されば送ります。)

正整数 d に対し $\mathbf{t}(d)$ を、$d \equiv 0,\ 3\ mod\ 4$ なら

$$\mathbf{t}(d) = \sum_{O \supseteq O_d} \frac{2}{w_O} \sum_{[\Lambda_O]} \left(j(\Lambda_O) - 744\right),$$

$d \equiv 1,\ 2\ mod\ 4$ なら $\mathbf{t}(d) = 0$ で定義し、さらに $\mathbf{t}(0) = 2, \mathbf{t}(-1) = -1$, 他の負正数 d についてはすべて $\mathbf{t}(d) = 0$ とする。ここで上のはじめの和は O_d を含む虚二次整環 O （有限個）をわたり、w_O は O の単数の個数、次の和は proper O ideal class group の代表 lattice (O の類数個）をわたる。j の値から 744 を引いているが、こうしないとあとの話がうまくないのであって、不思議といえば不思議である。この $\mathbf{t}(d)$ は $-d$ が所謂基本判別式（O_d が極大整環）で、-3 でも -4 でもなければ、$(w_{O_d} = 2)$ 代数的整数 $j(O_d) - 744$ のトレースにほかならない。このとき、

定理 (Zagier)　関数 $g(\tau) := \sum_{d=-1}^{\infty} \mathbf{t}(d)q^d$ は $\mathbf{H}$ 上正則な $\Gamma_0(4)$ に関する weight $\frac{3}{2}$ の modular form になる。

証明には古典的な道具立て (modular equation など）しか使わず、面白いものだが、上述のようにまだ書き上げられてないようである。

1.5 Singular moduli と Fourier 係数

前節に述べた Zagier の結果から $j(\tau)$ の Fourier 係数について興味ある公式を導くことが出来る。以下に述べる定理の公式がそれで、Fourier 係数を singular moduli により有限和の形で表わす。素朴に考えて、CM 点は $\mathbf{H}$ 内に稠密にあるからそこでの値で $j(\tau)$ は決まってしまう、だから Fourier 係数も singular moduli で表せても一向不思議はない、と、かねがね思ってはいたが、実際そういう表示式があったのである。(やはり想い続けるのが大事らしい。) これは非常に面白いと思うが、今のところその深い意味 (あるとして) がよく分からない。しかし少なくとも 、G. Shimura が非常に一般的なクラスの保型関数について証明した原理——保型関数の二通りの数論性、つまり Fourier 係数が $\bar{\mathbf{Q}}$ に入ることと CM 点での値が $\bar{\mathbf{Q}}$ に入ること、が同値であること——の一方向、CM 点 $\longrightarrow$ Fourier 係数、を explicit な形で与えたもの、といいうる。(Fourier 係数の代数性から CM 点での代数性を導く方向が、古典的な、modular equation の対角制限を使った singular moduli の代数性の証明である。) これが Moonshine と CM を結ぶかけ橋になるとか、そんなことでもあれば素晴しいが、と、これは全くの夢物語。

定理 (Kaneko, 1996) c_n $(n \geq 1)$ を $j(\tau)$ の Fourier 展開の q^n の係数とし、$\mathbf{t}(d)$ は前節の通りとする。このとき、

$$c_n = \frac{1}{n}\left\{\sum_{r\in\mathbf{Z}} \mathbf{t}(n-r^2) + \sum_{r\geq 1, odd}\Big((-1)^n \mathbf{t}(4n-r^2) - \mathbf{t}(16n-r^2)\Big)\right\}$$

が成り立つ。(右辺は実質有限和である。)

注意として、$\mathbf{t}(d)$ は次の漸化式を満たし (Zagier) 、従って初等的に (虚数乗法を離れて) 計算できる:

$$\begin{aligned} \mathbf{t}(4n-1) &= -a_n - \sum_{2\leq r\leq\sqrt{4n+1}} r^2 \mathbf{t}(4n-r^2), \\ \mathbf{t}(4n) &= -2 \sum_{1\leq r\leq\sqrt{4n+1}} \mathbf{t}(4n-r^2) \quad (n\geq 0) \end{aligned}$$

ここに $a_0 = 1,\ a_n = 240\sum_{d|n} d^3$ $(n \geq 1)$ である。

例: $\mathbf{t}(3) = -248,\ \mathbf{t}(4) = 492,\ \mathbf{t}(7) = -4119,\ \mathbf{t}(8) = 7256,\ \mathbf{t}(11) = -33512,\ \mathbf{t}(12) = 53008,\ \mathbf{t}(15) = -192513,\ \mathbf{t}(16) = 287244,\ \ldots$

$c_1 = 2\mathbf{t}(0) - \mathbf{t}(3) - \mathbf{t}(7) - \mathbf{t}(15) = 196884,\ c_2 = \frac{1}{2}(\mathbf{t}(-1) - \mathbf{t}(23) - \mathbf{t}(31)) = \frac{1}{2}(-1 - (-3493982) - (-39493539)) = 21493760,\ \ldots$

定理の証明であるが、前節 Zagier の定理を使うことにより、両辺を n 倍したものを weight 2 の modular forms の間の等式 (左辺は $\dfrac{1}{2\pi i}\dfrac{d}{d\tau}j(\tau)$) の q^n の係数を取り出したものとみなすことが出来、そう書いてしまえば、最初の数項の一致を確かめるだけで証明に

なる。(実はこうして証明される公式は

$$c_n = \frac{1}{n}\sum_{r\in\mathbf{Z}}\left\{\mathbf{t}(n-r^2) - \frac{(-1)^{n+r}}{4}\mathbf{t}(4n-r^2) + \frac{(-1)^r}{4}\mathbf{t}(16n-r^2)\right\}$$

であって、定理はこれを上の $\mathbf{t}(d)$ の漸化式を使って変形してある。) はじめにも述べたように、証明をつけてみても意味はもう一つ良くわからない。

2 Supersingular j invariants

2.1 定義

今度は標数 $p>0$ の有限体の代数閉包 $\bar{\mathbf{F}}_p$ 上で定義された楕円曲線 E を考えよう。このとき E の準同型環は虚 2 次整環か、∞ と p でのみ分岐する $\mathbf{Q}$ 上の四元数環の極大整環に同型になり、その区別は閉体上の同型類、つまり j 不変量のみによって決まる。前者の場合を ordinary 後者を supersingular と称する。言葉からもわかるように、ordinary なものが大多数である。準同型環が普通より大きくなる、という意味で、$\mathbf{C}$ 上の場合の CM 型に対応するのが supersingular であろう。CM 型のときその j 不変量は虚 2 次体上 abelian になるという、いわば制約がついたと同じく、supersingular な楕円曲線の j 不変量は必ず素体上の 2 次拡大 $\mathbf{F}_{p^2}$ に入る (Deuring)。したがって特に supersingular な楕円曲線の閉体上の同型類は有限個しかない。ここに A. Ogg による面白い観察がある。素数 p によっては、その標数の supersingular な楕円曲線の j 不変量が全て素体 $\mathbf{F}_p$ に入ることがあるが、そういう p は有限個で (これは証明される) そのリストが丁度 Monster 単純群の位数を割る素数の全体に一致するというのである。有限個しかないのだから並べて見れば”証明”はされるが、何故一致するかを説明する理論はいまのところ無いようである。“Moonshine” から考えても、ただの偶然の一致とは思えないのであるが。Hideji Ito は modular equation の膨大な計算から、この “Monster primes” を法とする、modular equation の係数の間のある興味深い合同式を発見した。これもこの”一致”から説明がつく。ここでは省略するが、関連文献をあげておいたのでご覧になられたい。

2.2 CM liftings

表題からは canonical lifting の話を連想される方が多いかもしれないが、その話ではない。

N. Elkies はその学位論文で、虚数乗法を持たない有理数体上の楕円曲線が supersingular reduction primes を無限個もつことを初めて示した。(その論文は K. Rubin が Tate-Shafarevich 群の有限性を初めて (ある場合に) 証明した論文と並んで Inventiones に載っている。9 年前のことである。) このような素数の密度はあとに述べる Lang-Trotter 予想によると x^2+1 型の素数の密度と同じ order で、この型の素数の無限性の方はまだ示されてないと思うから、楕円曲線の持つ構造の豊かさ故に証明が可能であったのだろうと思われる。その Elkies の証明は大体こういうことである。$E/\mathbf{Q}$ を non-CM, $j_0\in\mathbf{Q}$ をその j 不変量とし、有理数 $P_d(j_0)$ を考える。E は non-CM だからこれは 0 ではない。今素数 p

が $P_d(j_0)$ の分子に現れるとすると、$E\ mod\ p$ と、$\mathbf{Q}(\sqrt{-d})$ を CM にもつある楕円曲線の $mod\ \bar{p}$ ($\bar{p}$: p のある延長）が同じ j 不変量を持つことになる。Deuring の理論によると後者は p が $\mathbf{Q}(\sqrt{-d})$ で完全分解しなければ supersingular である。従って、d をいろいろ動かしたとき $p|(P_d(j_0)$ の分子) かつ $\left(\frac{-d}{p}\right) \neq 1$, なる p が無限個見つかることを示せばよい。Elkies はこれを類多項式の性質を巧妙に用いることにより実際に証明したのである。

さて今、有理数体上の楕円曲線 E に対して

$$\pi_E^{s.s}(x) := \{p \leq x | E\ mod\ p \ \text{が supersingular}\}$$

とおく。E は虚数乗法を持たないとする。Elkies の結果は

$$x \to \infty \text{ のとき } \pi_E^{s.s}(x) \to \infty$$

ということに外ならない。この $\pi_E^{s.s}(x)$ の order については S. Lang と H. Trotter によって

$$\pi_E^{s.s}(x) \sim c_E \frac{\sqrt{x}}{\log x} \quad (x \to \infty,\ c_E \text{ はある正定数})$$

と予想されている (1976)。しかし Elkies の証明から得られる $\pi_E^{s.s}(x)$ の lower bound は GRH (Generalized Riemann Hypothesis) を仮定しても

$$\pi_E^{s.s}(x) \gg \log\log x$$

程度である。ところで彼の証明のある部分は定量的に精密化出来て (Kaneko, 1989) 、それは lower bound の改良には役立たないのだが、$\pi_E^{s.s}(x)$ の次のような上からの評価（無条件）が得られる。

定理 (Elkies-(R. Murty), 1991)　$E/\mathbf{Q}$ は虚数乗法を持たない、とすると

$$\pi_E^{s.s}(x) = O(x^{3/4}).$$

この評価は偶然（か、何か理由があるのか？）J.-P. Serre (1981) が GRH のもとに与えた評価と同じになっている。もしかすると上の証明を GRH のもとで改良して、より良い評価を得ることが出来るのかもしれないが、わからない。

2.3 Non-CM liftings

こんどは supersingular j 不変量の “non-CM lifting” を考える。そのとき、ひとつの不変量の持ち上げを考えても（多分）面白くないので、次のような対象を考え、その有理数体上への持ち上げを考える。

$$ss_p(j) := \prod_{E/\bar{\mathbf{F}}_p,\ supersingular} (j - j(E)) \qquad \in \quad \mathbf{F}_p[j]\ .$$

これは $\mathbf{F}_p$ 上の j を変数とする monic 多項式で、その根が丁度標数 p の supersingular j 不変量全体になっているものである。

例: $ss_2(j) = j,\ ss_3(j) = j,\ ss_5(j) = j,\ ss_7(j) = j-6,\ ss_{11}(j) = j(j-1),\ ss_{13}(j) = j-5,\ ss_{17}(j) = j(j-8),\ \ldots,\ ss_{37}(j) = (j-8)(j^2-6j-6),\ \ldots$

さて一般に $SL_2(\mathbf{Z})$ の modular form $f(\tau)$ に対して、

$$\widehat{f}(j) := \prod_{\tau_0 \in \mathbf{H},\ f(\tau_0)=0} (j - j(\tau_0))$$

とおく。ここで積は $f(\tau)$ の上半平面における零点の $SL_2(\mathbf{Z})$ 同値類の代表をわたるものとする。保型因子 "$c\tau + d$" は上半平面上で零になることはないから、零点の $SL_2(\mathbf{Z})$ 同値類というのが well-defined になり、f が恒等的に零でない限り零点の同値類は有限個故 $\widehat{f}(j)$ は $\mathbf{C}$ 上の j を変数とする monic 多項式となる。今特に Eisenstein 級数

$$E_k(\tau) := 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n \quad (B_k = k\text{-th Bernoulli number},\ \sigma_{k-1}(n) = \sum_{d|n} d^{k-1})$$

を考えると、次のことが知られている。

定理 (Herglotz (1922), Deligne)　p を 5 以上の素数とするとき、

$$\widehat{E_{p-1}}(j)\ mod\ p = ss_p(j)$$

が成り立つ。

文献にあげた Serre の "Congruences et formes modulaires" ではこれを Deligne の定理としているが、 essential には Herglotz に遡ることが出来るように見える（ただし Herglotz の頃はまだ "supersingular elliptic curve" の概念も無いから適当な解釈が必要だが)。その要点は von-Staudt の定理から来るところの $E_{p-1}(\tau)$ の q 展開の合同式 $E_{p-1} \equiv 1\ mod\ p$ にある。

これでわかるように Eisenstein 級数の系列は全体として $ss_p(j)$ の simultaneous な持ち上げを与えている。($p-1$ の形でない偶数についても何らかの合同関係によりある $ss_p(j)$ と結び付く。）ところが、全く別の系列で同じように $ss_p(j)$ の持ち上げを与えているものがある。ひとつは Atkin によるある直交多項式で、もうひとつは Zagier-Kaneko による "hypergeometric modular form" である。後者を先に、しかも天下り的に述べてしまおう。

$E_2(\tau)$ を weight 2 の Eisenstein 級数とする。これは先に書いた Eisenstein 級数の式で $k = 2$ としたもので、modular form ではないが、$\mathbf{H}$ 上の正則関数である。これが "判別式" $\Delta(\tau)$ の対数微分になっていることに注意すれば $SL_2(\mathbf{Z})$ の元による変換則も簡単にわかる。今、２階の微分方程式

$$f''(\tau) - \frac{k+1}{6} E_2(\tau) f'(\tau) + \frac{k(k+1)}{12} E_2'(\tau) f(\tau) = 0 \quad (\ ' = \frac{1}{2\pi i} \frac{d}{d\tau})$$

を考えると、k が 4 以上の偶数で、$k \not\equiv 2\ (mod\ 3)$ ならば、この方程式の解として $SL_2(\mathbf{Z})$ の weight k の modular form $F_k(\tau)$ が定数倍を除き一意的に存在することが証明できる。これについて再び

定理 (Zagier-Kaneko)　p を 5 以上の素数とするとき、

$$\widehat{F_{p-1}}(j)\ mod\ p = ss_p(j)$$

が成り立つ。

$F_k(\tau)$ はまた、ある canonical な２階の微分作用素（を $E_4(\tau)$ で割ったもの）からくる、weight k の modular form の空間に働く準同型の、cusp form ではない唯一の固有関数として（定数倍を除き）特徴づけることが出来る。Eisenstein 級数が 、Hecke 作用素の同時固有関数で cusp form でない唯一のもの、として特徴づけられることを思い出そう。

$ss_p(j)$ が２階の微分方程式（$\mathbf{F}_p(j)$ 上）を満たすことは J.-I. Igusa 以来知られていて、その方程式の”良い”lifting が上の方程式になっている。それが定理のひとつの説明である。面白いことに、全く同じ微分方程式が K. Saito, Ikuo Satake らが研究されている”特異点の変形理論”に関する話からも出てくる。この辺の事情はまだよく理解してないのだが、色々と調べることがありそうである。

次に Atkin の直交多項式であるが、これは次のようにして定義される。まず、多項式環 $\mathbf{C}[j]$ を $j = j(\tau)$ を通して $SL_2(\mathbf{Z})$ の weight 0 の modular function で $\mathbf{H}$ 上正則、cusp では極を許すもの、の全体と同一視する。これにより $\mathbf{C}[j]$ には Hecke 作用素 $\{T_n\}$ が働く。

定理 (Atkin) (i) $\mathbf{C}[j]$ 上の非退化な内積 $(\ ,\ )$ で $(f|T_n, g) = (f, g|T_n)$ がすべての $f, g \in \mathbf{C}[j],\ n \geq 0$ について成り立つものが存在する。
(ii) この内積に関する直交多項式系を $\{A_n(j)\}_{n\geq 0}$, $A_n(j)$ は n 次 monic, とする。$A_n(j) \in \mathbf{Q}[j]$ であり、さらに p を素数（今度は $2, 3$ でもよい）、$n_p = deg\ ss_p(j)$ とするとき、

$$A_{n_p}(j)\ mod\ p = ss_p(j)$$

が成り立つ。

例: $A_1(j) = j - 720,\ A_2(j) = j^2 - 1640j + 269280,\ A_3(j) = j^3 - \frac{12576}{5}j^2 + 1526958j - 107765856,\ A_4(j) = j^4 - 3384j^3 + 3528552j^2 - 1133263680j + 44184000960,\ \ldots$

この内積は具体的には

$$(f(j), g(j)) = Res_{q=0} f(j(q))g(j(q))E_2(q)\frac{dq}{q}$$

で与えられる。ここに、$j(q),\ E_2(q)$ はそれぞれ $j(\tau),\ E_2(\tau)$ の Fourier 展開級数を形式的 Laurent 級数とみたものである。またこれを

$$(f(j), g(j)) = \int_0^{1728} f(j)g(j)\mu(j)dj\ \ (\mu(j) \text{はある正の関数})$$

という、古典的な直交多項式を定める内積の形に書き直すことも出来る。大事なことは、この内積が“ Hecke 作用素が self-adjoint”ということから定数倍を除き一意に決まってしまう点である（ただし考える内積は（古典的な場合がすべてそうであるように）二つの元

の積にのみ依存するとする)。したがって直交多項式系 $\{A_n(j)\}_{n\geq 0}$ も Hecke 作用素から canonical に決まっていると言うことが出来る。

この $A_n(j)$ や先の $F_k(\tau)$ は超幾何級数や Jacobi 多項式などと関係して、あるいは解釈されて、面白い性質がいろいろあるがここでは省略するとし、ひとつだけ、ずっと不思議に思っていることを次の節で述べる。ところで、何故にこのようにいろいろと $ss_p(j)$ の持ち上げを考えるか。志村先生の”考えて何が悪いか”というのも答え方であろうが、ひとつには §2.3 で述べた supersingular reduction primes の分布の研究に役立つかもしれない、という希望、もうひとつは、Deuring が虚数乗法を持つ楕円曲線の L 関数の、、、、、、いや、やはり”考えて何が悪いか”ですますとしよう。

supersingular j 不変量と超幾何級数ということに関しては、70 年代はじめの Y. Ihara の一連の研究(標数 p のモジュラー関数体に付随したある不変微分、標数 p の Schwarz 微分の理論、etc.)がまだまだ未知の”何か”を蔵しているように感じているのだが、今後の課題ということにしたい。

2.4 Zeros of modular forms

前節で扱つた三つの対象 $\widehat{E}_k(j),\ \widehat{F}_k(j),\ A_n(j)$ はすべて、適当な entry の根を適当な素数で reduce すると supersingular j 不変量を与へるといふ性質をもつたのだが、標数 0 でも次の共通の性質を持つ。

定理　$\widehat{E}_k(j),\ \widehat{F}_k(j),\ A_n(j)$ の根はすべて実単根で、区間 [0,1728] にある。

これは $E_k(\tau)$ については F.K.C. Rankin(有名な R.A. Rankin の娘ださう)と Swinnerton-Dyer の結果 (1970) であり、他の場合は直交多項式の一般論から簡単に導ける。これはしかし何を意味してゐるのであらうか?更にもうひとつ、

$$(j-744)|T_n \text{ も同じ性質を持つ} \quad \text{(H. Ninomiya -(T. Asai-Kaneko))}$$

(744 は $0<a<1728$ なる任意の a でよい)。このことを使つて例へば $\dfrac{1}{j(\tau)}$ の Fourier 係数の符号が交代的であることを証明することが出来る。何にせよこの零点のことは mysterious と思ふのだが如何であらうか。

3　超越数論の話題から

この章では主として、今年(1996 年)の 5 月に日本に来られた M. Waldschmidt さんから伺った話を紹介する。

j 関数の値の超越性について次の T. Schneider の定理は良く知られている。

定理 (Schneider, 1937)　$\tau_0 \in \mathbf{H}$ が代数的でかつ虚二次数ではないとすると $j(\tau_0)$ は超越的である。

最近、τ ではなく q を変数にとった時の j の値の超越性について進展があった。$J(q)$ で $j(\tau)$ の q 展開を表し、これを $q \mapsto J(q)$ なる関数とみよう。

定理 (Barré-Sirieix, Diaz, Gramain and Philibert, 1996)　$0 < |q| < 1,\ q \in \mathbf{C}$ または $0 < |q|_p < 1,\ q \in \mathbf{C}_p$ とする。もし q が代数的ならば $J(q)$ は超越的である。

これは複素数のときは Mahler, p-adic case は Manin が予想していたもので、後者は p 進 L 関数の零点への応用を持つ。

複素数の場合のこの定理はより最近の次の結果に含まれる。

定理 (Nesterenko, 1996)　$0 < |q| < 1,\ q \in \mathbf{C}$ とする。体 $\mathbf{Q}(q, E_2(q), E_4(q), E_6(q))$ の ($\mathbf{Q}$ 上の) 超越次数は 3 または 4 である。

ここに、$E_2(q), E_4(q), E_6(q)$ はそれぞれ weight 2, 4, 6 の Eisenstein 級数の値である。$J(q) = 1728E_4(q)^3/(E_4(q)^3 - E_6(q)^2)$ であるから、q が代数的ならば $J(q)$ は代数的ではありえない（超越次数が 2 以下になってしまう）。

この定理を使うと例えば $q = e^{-2\pi}$ $(\tau = i)$ として、$\pi,\ e^{\pi},\ \Gamma(1/4)$ が代数的に独立であることなどが出てくる。π と e^{π} が独立、というのも以前は知られていなかったそうである。

ところで、これらの定理とは直接関係はないのであるが、超越数論で "four exponentials conjecture" という未解決の予想があって、正しいと信じられているらしい。どういう予想かというと、λ_i $(1 \le i \le 4)$ を $e^{\lambda_i} \in \bar{\mathbf{Q}}$ なる複素数とし、これらが $\lambda_1\lambda_4 - \lambda_2\lambda_3 = 0$ を満たすとすると、$\dfrac{\lambda_1}{\lambda_2} \in \mathbf{Q}$ か $\dfrac{\lambda_1}{\lambda_3} \in \mathbf{Q}$ であろう、というものである。これ以上の解説は省略させてもらって（実は出来ない）これから出る帰結を紹介しよう。

その１ (D. Bertrand) "four exponentials conjecture" が正しいとすると、関数 $q \mapsto J(q)$ は $\bar{\mathbf{Q}} \cap \{q \in \mathbf{C} |\ 0 < |q| < 1\}$ 上単射である。

その２ (G. Diaz) "four exponentials conjecture" が正しいとすると、単位円 $\{z \in \mathbf{C} |\ |z| = 1\}$ 上で関数 $e^{2\pi iz}$ の値が代数的になるのは $z = \pm 1$ に限る。

どちらも一寸異様な印象を与える。後者は全く j 関数とは関係がないが、その証明を少しだけ一般化すると次のことが言える。

その３ "four exponentials conjecture" が正しいとすると、"$j(\tau) \in [0, 1728]$ かつ $q = e^{2\pi i\tau} \notin \mathbf{R} \Rightarrow q \notin \bar{\mathbf{Q}}$" が成り立つ。

これと先の Nesterenko の定理を眺めていると、区間 $[0, 1728]$, 特に arithmetic な modular form の零点での j value （それは代数的である）がこの区間に入ることには何か特別な意味でもあるか、と、少しは思えてくる。実はこれを言いたいが為に自分にはまだ remote な超越数論の話題を衒って述べて来たのだが、いい加減ボロが出そうなのでこの辺でやめるといたしましょう。

最後に文献を[†]

- 楕円モジュラー関数についての原典
  - R. Dedekind: *Schreiben an Herrn Borchardt über die Theorie der elliptischen Modulfunktionen,* Jour. für reine und angew. Math. **83** (1877) 265–292. （全集1巻 174–201) （とても読みやすい）
  - F. Klein: *Über die Transformation der elliptischen Funktionen und die Auflösung der Gleichungen fünften Grades,* Math. Annalen **14** (1878/79)（全集3巻 13–75)
  - A. Hurwitz: *Grundlagen einer independenten Theorie der elliptischen Modulfunktionen und Theorie der Multiplikator-Gleichungen erster Stufe,* Math. Annalen **18** (1881) 528–592 （全集1巻 1-66)
- 楕円関数、モジュラー形式、楕円モジュラー関数についての一般書（これらについてはあまり沢山あるので3冊だけ）
  - 竹内端三: “楕圓函數論”、1936、 岩波全書 （再版されているはず）
  - J.P. Serre: “数論講義”、1979、岩波書店 （これは絶版かも）
  - D.A. Cox: “Primes of the form $x^2 + ny^2$”, 1989, John Wiley Sons （これは良い本)
- $j(\tau)$ の Fourier 係数の解析的公式
  - H. Petersson: *Über die Entwicklungskoeffizienten der automorphen Formen,* Acta Math. **58** (1932), 169–215.
  - H. Rademacher: *The Fourier coefficients of the modular invariant $J(\tau)$,* Amer. J. Math. **60** (1938), 501–512.
  - H. Rademacher: *The Fourier series and the functional equations of the absolute modular invariant $J(\tau)$,* Amer. J. Math. **61** (1939), 237–248.
  - M.I. Knopp: *Rademacher on $J(\tau)$, Poincaré series of nonpositive weights and the Eichler cohomology,* Notices AMS **37-4** (1990), 385–393. (Rademacher の仕事の survey)

[†] もとより完璧を期したものではありません。大事な文献を見落としてないか、と危惧しますが、ここに挙げてある文献のそのまた引用文献、、、と辿って頂けたら良いかと思います。お気づきのこと（本文も含め）ございましたらご教示下さい。

- $j(\tau)$ の Fourier 係数の合同式、Atkin の予想
  - D.H. Lehmer: *Properties of the coefficients fo the modular invariant $J(\tau)$,* Amer. J. Math. **64** (1942), 488–502.
  - J. Lehner: *Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$,* Amer. J. Math. **71** (1949), 136–148.
  - J. Lehner: *Further congruence properties of the Fourier coefficients of the modular invariant $j(\tau)$,* Amer. J. Math. **71** (1949), 373–386.
  - M. Newman: *Congruences for the coefficients of modular forms and for the coefficients of $j(\tau)$,* Proc. Amer. Math. Soc. **9** (1958), 609–612.
  - O. Kolberg: *Congruences for the coefficients of the modular invariant $j(\tau)$,* Math. Scand. **10** (1962), 173–181.
  - A.O.L. Atkin and J.N. O'Brien: *Some properties of $p(n)$ and $c(n)$ modulo powers of* 13*,* Trans. Amer. Math. Soc. **126** (1967), 442–459.
  - A.O.L. Atkin: *Congruence Hecke operators,* Proc. Symp. Pure Math. **12** (1969), 33–40.
  - O. Kolberg: *On the Fourier coefficients of the modular invariant $j(\tau)$,* Årb. Univ. Bergen, Mat.-Naturv. Serie **3** (1969), 3–8.
  - M. Koike: *Congruences between modular forms and functions and applications to the conjecture of Atkin,* J. Fac. Sci. Univ. Tokyo **20** (1973), 129–169.
- Monstrous Moonshine 関係
  - J.H. Conway and S.P. Norton: *Monstrous Moonshine,* Bull. London Math. Soc. **11** (1979), 308–339. （Monstrous Moonshine の原典）
  - I.B. Frenkel, J. Lepowsky and A. Meurman: "Vertex Operator Algebras and the Monster", Pure and Applied Mathematics. **134**, Academic Press, 1988.
  - R. Borcherds: *Monstrous moonshine and monstrous Lie superalgebras,* Invent. Math. **109** (1992), 405–444.
  - J.H. Conway: *Monster and Moonshine,* Math. Intelligencer **2** (1980), 165–171. (面白い読み物)
  - 小池正夫: Moonshine–単純群と保型関数の不思議な関係–, " 数学" 40 巻 3 号 (1988).
  - F.J. Dyson: *Unfashionable Pursuits,* Math. Intelligencer **5-3** (1983), 47–54. (翻訳が " 流行らない研究のすすめ "、 数学セミナー 1984 年 4 月号、にある。面白く、また心強くもある)
- 虚数乗法論
  - L. Kronecker: 全集 IV, V 巻の様々な論文

- G. Pick: *Ueber die complexe Multiplication der elliptischen Functionen I, II,* Math. Annalen **25** (1885) 433–447, 同 **26** (1886), 219–230.
- H. Weber: "Leherbuch der Algebra", 第 III 巻 1908, Chelsea.
- G. Shimura: "Introduction to the Arithmetic Theory of Automorphic Functions", Iwanami Shoten and Princeton Univ. Press, 1971. (adele による定式化で書かれた最初の本)
- 上述 Cox の本
- J.H. Silverman: "Advanced Topics in the Arithmetic of Elliptic Curves", Springer GTM151, 1994.
- S.G. Vladut: "Kronecker's Jugendtraum and modular functions", Gordon and Breach, 1991. (歴史に詳しい)

- Borcherds の無限積、$j(\tau)$ の Fourier 係数の代数公式
  - R. Borcherds: *Automorphic forms on* $O_{s+2,2}(\mathbf{R})$ *and infinite products,* Invent. Math. **120** (1995), 161–213.
  - M. Kaneko: *The Fourier coefficients and the singular moduli of the elliptic modular function* $j(\tau)$, Mem. Fac. Eng. and Design, KIT **44** (1996), 1–5.
  - D. Zagier: *Traces of singular moduli,* 準備中

- 保型形式の数論性
  - 志村五郎: 種々の zeta 関数の値と周期の数論性について、 「数学」第 45 巻 2 号 (1993 年 4 月 春季号)、 111–127. (及びそこに引用されている諸論文)

- Supersingular j invarinat 関連
  - G. Herglotz: *Über die Entwicklungskoeffizienten der Weierstraßschen* $\wp-$*Funktion,* Leipziger Ber. **74** (1922), 269–289 (全集 436–456).
  - M. Deuring: *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper,* Abh. Math. Sem. Hamburg **14** (1941), 197–272 . (有限体上の楕円曲線、特に supersingular curve について何か書く人は必ず引用する " 定番 ")
  - J.-I. Igusa: *Class number of a definite quaternion with prime discriminant,* Proc. N. A. S. **44** (1958), 312–314.
  - Y. Ihara: *An invariant multiple differential attached to the field of elliptic midular functions of characteristic p,* Amer. J. Math. **93** (1971), 139–147.
  - Y. Ihara: *Schwarzian equations,* J. of the Fac. of Sci. Univ. Tokyo **21-1** (1974), 97–118.
  - Y. Ihara: *On the differentials associated to congruence relations and the Schwarzian equations defining uniformizations,* J. of the Fac. of Sci. Univ. Tokyo **21-3** (1974), 309–332.

- J.P. Serre: *Conguences et formes modulaires,* Sém. Bourbaki 1971/72, **416** (全集 95).
- J.P. Serre: *Quelques applications du théorème de densité de Chebotarev,* Publ. Math. I.H.E.S. **54** (1981), 123–201 (全集 125)
- N. Elkies: *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbf{Q}$*,* Invent. Math. **89** (1987), 561–567.
- M. Kaneko: *Supersingular $j-$invariants as singular moduli mod p,* Osaka J. Math. **26** (1989), 849–855.
- N. Elkies: *Distribution of supersingular primes,* Astérisque **198-199-200** (1991), 127–132.
- M. Kaneko and D. Zagier: *Supersingular $j-$invariants, hypergeometric series, and Atkin's orthogonal polynomials,* 準備中

- "Monster primes", Modular equation の係数
  - A. Ogg: *Automoprphismes de Courbes Modulaires.,* Sém. Delange-Pisot-Poitou 16e année **7** (1975), 1–8. （"一致"を説明した人には "Jack Daniels" 一本差し上げる、と）
  - Hideji Ito: *Computation of the modular equation,* Proc. Japan Acad., **71** (1995), 48–50.
  - M. Kaneko: *On Ito's observation on coefficients of the modular polynomial,* Proc. Japan Acad. **72** (1996), 95–96.

- Eisenstein series の零点、他の零点
  - R.A. Rankin: *The zeros of Eisenstein series,* Publ. Ramanujan Inst. **1** (1969), 137–144. （Atkin の内積はこの論文がヒントになっている）
  - F.K.C. Rankin and H.P.F. Swinnerton-Dyer: *On the zeros of Eisenstein series,* Bull. London Math. Soc. **2** (1970), 169–170. （Atkin 言うところの "embarrassingly simple" proof）
  - R.A. Rankin: *The zeros of certain Poincaré series,* Compositio Math. **46-3** (1982), 255–272.
  - T. Asai, M. Kaneko and H. Ninomiya: *On the signs of the Fourier coefficients of* $1/j(\tau)$*,* プレプリント

- 超越数論関連
  - T. Schneider: *Arithmetische Untersuchungen elliptischer Integrale,* Math. Ann. ,**113** (1937), 1–13.
  - K. Mahler: *Remarks on a paper by W. Schwarz,* J. Number Th., **1** (1969), 512–521.

– Yu. I. Manin: *Cyclotomic fields and modular curves,* Russian Math. Surveys, —bf 26 (1971), 7–78.

– K. Mahler: *On the coefficients of the* 2^n-th *transformation polynomial for* $j(w)$*,* Acta Arith., **21** (1972), 89–97.

– K. Barré-Sirieix, G. Diaz, F. Gramain and G. Philibert: *Une prouve de la conjecture de Mahler-Manin,* Invent. Math. **124** (1996), 1–9.

– Y. Nesterenko: *Modular functions and transcendencs problems,* C. R. Acad. Sci. Paris **322-1** (1996), 909–914.

– M. Waldschmidt: *Sur la nature arithmétique des valeurs de fonctions modulaires,* to appear in Sém. Bourbaki 49ème année, 1996–97, n° 824.