ARGOS seminar on intersections of modular correspondences, Astérisque **312** (2007) の紹介

服部 新
北大理学研究院 3-601
shin-h@math.sci.hokudai.ac.jp

平成 19 年 10 月 6 日

※ B. H. Gross, K. Keating, *On the intersection of modular correspondences*, Invent. Math **112** (1993), 225-245 の解説本

1 Statement

$\varphi_m(X, Y)$: modular polynomial

$$\begin{aligned}\varphi_m(j(E), j(E')) &= \prod_{[E_1' \to E']:\text{isog. of deg}=m} (j(E) - j(E_1')) \\ &= \prod_{A \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathrm{M}_2(\mathbb{Z}):\det(A)=m} (j(\tau) - j(A\tau')) \\ &\in \mathbb{Z}[j, j']\end{aligned}$$

$T_m := V(\varphi_m) \subseteq S := \mathbb{A}^1_{\mathbb{Z}} \times \mathbb{A}^1_{\mathbb{Z}}$

ここで, $\mathbb{A}^1_{\mathbb{Z}} \times \mathbb{A}^1_{\mathbb{Z}}$ は j-invariant により, elliptic curve のペアを分類する stack の coarse moduli scheme と思う.

このような divisor 3 つの算術的交点数

$$(T_{m_1}, T_{m_2}, T_{m_3}) := \log(\sharp\mathbb{Z}[j, j']/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3}))$$

を考える.

定理 1.1 (主定理 (Gross-Keating)) *(i) divisor $T_{m_1}, T_{m_2}, T_{m_3}$ が intersect properly $\Longleftrightarrow$ m_1, m_2, m_3 を同時に represent する positive definite binary 二次形式 $/\mathbb{Z}$ が存在しない.*

(ii) このとき, intersection $T_{m_1} \cap T_{m_2} \cap T_{m_3}$ は S の閉点からなる次のような有限集合の上にある.

$$\{[E, E'] | p < 4m_1m_2m_3 \text{なる素数に対する}, \bar{\mathbb{F}}_p \text{ 上の } \textit{supersingular elliptic curve} \text{ のペア } \}$$

(iii)

$$(T_{m_1}, T_{m_2}, T_{m_3}) = \sum_{p < 4m_1m_2m_3} n(p) \log(p).$$

但し

$$n(p) = \frac{1}{2}\sum_{Q} \alpha_p(Q) \cdot (\prod_{l|\Delta(Q), l\neq p} \beta_l(Q)).$$

ここで

- $\sum_Q$ は, $\mathbb{Z}$ 上の *positive definite ternary* 二次形式 Q で, 対角成分が (m_1, m_2, m_3) であり, かつ任意の $l \neq p$ に対して $Q \otimes_{\mathbb{Z}} \mathbb{Q}_l$ が *isotropic* であるもの全体をわたる和
- $\alpha_p(Q)$ は $Q \otimes \mathbb{Z}_p$ の同型類で決まるある *invariant (「universal deformation ring* における *divisor* の交点数」*)*
- $\beta_l(Q)$ は $Q \otimes \mathbb{Z}_l$ の $(\mathrm{M}_2(\mathbb{Z}_l), \det)$ に対する *local density* を *normalize* したもの
- $\Delta(Q)$ は Q の *determinant* を *normalize* したもの

用語は以下で説明する.

2 quadratic space の用語集

R は (unitary な) 可換整域で, 2 が zero-divisor でないものとする.

定義 2.1 R 上の quadratic space (M, Q) とは, 自由 R-加群 (of rank n) M と map $Q : M \to R$ の組で, 次の条件を満たすもの.

- $Q(rx) = r^2 Q(x)$ $(x \in M,\ r \in R)$
- $(x, y) := Q(x + y) - Q(x) - Q(y)$ が $M \times M \to R$: symmetric bilinear map を定める (とくに $(x, x) = 2Q(x)$)

注 2.2

- $m = 1, 2, 3, 4$ のときそれぞれ, unary, binary, ternary, quaternary quadratic space という.
- M の basis $x_1, \ldots, x_n$ を fix すると,

$$Q(t_1x_1 + \ldots + t_nx_n) = \sum_{i=1}^{n} \frac{1}{2}(x_i, x_i)t_i^2 + \sum_{i>j}(x_i, x_j)t_it_j$$

  と書ける. とくに $(x_i, x_i) \in 2R$, $(x_i, x_j) \in R$.

- $B_Q = \frac{1}{2}((x_i, x_j))_{i,j}$ とおくと,

$$B_Q \in \mathrm{Sym}_n^{\vee}(R) := \{(b_{i,j}) \in \mathrm{M}_n(R) |\ 対称行列で,\ b_{i,i} \in R, b_{i,j} \in \frac{1}{2}R\}$$

- R が標数 $\neq 2$ の体なら, (M, Q) には orthogonal basis が存在.
- $p \neq 2$ のとき, $\mathbb{Z}_p$ 上の quadratic space にも orthogonal basis が存在することが示せる. $p = 2$ のときはこれは成立しない ($\mathbb{Q}_2$ 上なら存在する).

定義 2.3

- (M, Q) が non-gedenerate (regular ともいう) とは, $\det(B_Q) \neq 0$ であること. これは $M \to \mathrm{Hom}_R(M, R)$ の injectivity と同値.

- (M,Q) が isotropic とは, $Q(x)=0$ となる $x\neq 0$ が存在すること. このような x が存在しないとき, (M,Q) を anisotropic という.

- $(M_1,Q_1)\to(M_2,Q_2)$: isometry とは, $f: M_1\to M_2$: R-linear injection で $Q_2\circ f=Q_1$ を満たすもの. surjective な isometry があるとき, これらを同型とか isometric とかと言い, $(M_1,Q_1)\simeq(M_2,Q_2)$ で表す.

- $\det(Q):=\det(B_Q) \bmod (R^\times)^2\in R/(R^\times)^2$ (つまり, basis の取り方の分だけ不定性 $(R^\times)^2$ がある).

- $\Delta(Q):=\frac{1}{2}\det((x_i,x_j)) \bmod (R^\times)^2\in R/(R^\times)^2$. つまり, (M,Q) が rank n だとすると, $\Delta(Q)=2^{n-1}\det(Q)$.

- $(M,Q_M),(N,Q_N)$: quadratic space, に対し

$$\mathrm{R}_N(M):=\sharp\mathrm{Isometry}((M,Q_M),(N,Q_N))$$

  とおき, N における M の representation number という.

3 local density

$(M,Q_M),(N,Q_N)$: $\mathbb{Z}_p$ 上の regular quadratic space, rank$=m,n$
それぞれ basis を取って, 行列 B_{Q_M},B_{Q_N} を考える. $r\geq 0$ に対し

$$\begin{aligned}A_{p^r}(M,N):&=\sharp\{X\in\mathrm{M}_{n,m}(\mathbb{Z}_p/p^r\mathbb{Z}_p)\mid {}^tXB_{Q_N}X-B_{Q_M}\in p^r\mathrm{Sym}_m^\vee(\mathbb{Z}_p)\}\\&=\sharp\{\sigma: M/p^rM\to N/p^rN\mid Q_N(\sigma(x))\equiv Q_M(x) \bmod p^r\}\end{aligned}$$

とおくと, $(p^r)^{\frac{m(m+1)}{2}-mn}A_{p^r}(M,N)$ は r が十分大で一定値になることが示せる. そこで

$$\alpha_p(M,N):=\lim_{r\to\infty}2^{-\delta_{m,n}}(p^r)^{\frac{m(m+1)}{2}-mn}A_{p^r}(M,N)$$

とおいて, これを M の N に対する local density と呼ぶ. (主定理に出てきた $\alpha_p(Q)$ とは別物)

注 3.1
- この定義は桂田先生の論文のものにあわせてあり, 北岡先生の教科書 (Arithmetic of quadratic forms) での定義とは normalization が異なる. そっちの本では「$\in p^r\mathrm{Sym}_m^\vee(\mathbb{Z}_p)$」(半整数行列) の代わりに「$\in p^r(2\cdot\mathrm{Sym}_m^\vee(\mathbb{Z}_p))$」(偶行列) を考えるので, $p=2$ のときに少しずれる. つまり,

$$\begin{aligned}\alpha_p(M,N)&=\alpha_p^{北岡}(M,N) \text{ if } p\neq 2\\ \alpha_2(M,N)&=2^{\frac{m(m+1)}{2}}\alpha_2^{北岡}(M,N)\end{aligned}$$

- $\alpha_p(M,N)\neq 0$ なら, $M\hookrightarrow N$: isometry, が存在することを示すことができる.

定義 3.2 Q を主定理で述べたような $\mathbb{Z}$ 上の quadratic space とするとき

$$\beta_l(Q):=\frac{1}{(1-\frac{1}{l^2})^2}\cdot\alpha_l(Q\otimes\mathbb{Z}_l,(\mathrm{M}_2(\mathbb{Z}_l),\det))$$

4　二次形式の Gross-Keating invariant

$\mathbb{Z}_p$ 上の階数 n の regular quadratic space (M, Q) を考える.

各 basis$\psi = \{\psi_1, \ldots, \psi_n\}$ に対し, ψ に関する Q の行列表示 $B_Q = (b_{ij}(\psi))_{ij}$ を考える. さらに,

$$S(\psi) := \{(y_1, \ldots, y_n) \in \mathbb{Z}^n \mid \begin{array}{l} y_1 \leq y_2 \leq \cdots \leq y_n \\ \frac{y_i + y_j}{2} \leq \mathrm{ord}_p(b_{ij}(\psi)) \end{array} \}$$

$$S := \cup_\psi S(\psi)$$

とおく. S には辞書式順序を入れる. つまり,

$$(y_1, \ldots, y_n) \leq (z_1, \ldots, z_n) \Leftrightarrow k \text{ を「} l < k \text{ ならば } y_l = z_l \text{」なる最大の数とするとき}, y_k \leq z_k$$

と定める. これによって S は全順序集合となり, (M, Q) の regularity から S には最大元が存在することが簡単に分かる. この最大元 $(a_1, \ldots, a_n)$ を, (M, Q) の **Gross-Keating invariant** と呼ぶ.

注 4.1

- $p \neq 2$ なら (M, Q) は diagonalizable である. つまり, M の basis $\psi_1, \ldots, \psi_n$ で,

  $$Q(x_1\psi_1 + \cdots + x_n\psi_n) = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2, \ \mathrm{ord}_p(\alpha_1) \leq \ldots \leq \mathrm{ord}_p(\alpha_n)$$

  を満たすものが存在. このとき, (M, Q) の Gross-Keating invariant $(a_1, \ldots, a_n)$ は

  $$a_i = \mathrm{ord}_p(\alpha_i)$$

  であることが示せる. $p = 2$ のときは, $\mathbb{Z}_2$ 上 diagonalizable でない quadratic space が存在するので, もう少し微妙になっている.

- 実際は, $a_1 = \min_{m \in M} \mathrm{ord}_p(Q(m))$ であることが示せるので, $a_i \geq 0$.

- $n = 3$ のとき, $a_1 \equiv a_2 \equiv a_3 (2)$ ならば, (M, Q) は isotropic であることが示せる.

5　主定理の証明の概略

主定理の (i), (ii) は難しくない. modular polynomial が closed fiber 上でも $\mathbb{C}$ 上と同様の moduli 解釈を持つことから従う. 以下主定理 (iii) について考える.

主定理の (ii) から, 三つの divisor $T_{m_1}, T_{m_2}, T_{m_3}$ が proper に交わっているとき, 問題の交点数は

$$(T_{m_1}, T_{m_2}, T_{m_3}) = \sum_{p < 4m_1m_2m_3} \sum_{[E, E']: \mathrm{ss.}/\bar{\mathbb{F}}_p} (T_{m_1}, T_{m_2}, T_{m_3})_{[E, E']}$$

と局所交点数の和に分解する.

$j_E = j(E)$, $j_{E'} = j(E') \in \bar{\mathbb{F}}_p$ とおき, $\tilde{j}_E$, $\tilde{j}_{E'}$ をそれらの $W = W(\bar{\mathbb{F}}_p)$ への lift とする. 極大イデアル

$$(p, j - \tilde{j}_E, j' - \tilde{j}_{E'}) \subseteq W[[j, j']]$$

での $W[[j, j']]$ の完備化を $R_0 := W[[j - \tilde{j}_E, j' - \tilde{j}_{E'}]]$ と書く ($S \times_{\mathbb{Z}} \mathrm{Spec}(W)$ の, 点 $(j_E, j_{E'})$ における完備局所環).

一方, pair (E,E') の universal deformation ring を R とおき, universal elliptic curve を $(\mathbb{E},\mathbb{E}')$ とする. 定義からこれは, 関手

$$\begin{aligned}((A,m)\text{：}W\text{ 上の Artin 局所環, 剰余体 }\bar{\mathbb{F}}_p) &\to (\mathrm{Set})\\ A &\mapsto \{[(\mathcal{E},i),(\mathcal{E}',i')]\}\end{aligned}$$

を pro-represent する元. ただし, 右辺は次のような集合.

- $\mathcal{E}$ は A 上の elliptic curve.
- $i:\mathcal{E}\times_A\bar{\mathbb{F}}_p\cong E$ は k 上の elliptic curve の同型 ($\mathcal{E}'$, i' も同様).
- $[(\mathcal{E},i),(\mathcal{E}',i')]$ はそれらの同型類の組.

elliptic curve は k 上 smooth projective だから, deformation は unobstructed で, E の universal deformation ring は W 上 $\dim_{\bar{\mathbb{F}}_p}\mathrm{H}^1(E,(\Omega^1_{E/\bar{\mathbb{F}}_p})^\vee)=1$ 変数の巾級数環と同型. したがって, W-同型 $R\cong W[[t,t']]$ が存在.

一方, E の universal deformation ring には次のように $\sigma\in\mathrm{Aut}(E)$ が作用している.

$$\sigma.[\mathcal{E},i]=[\mathcal{E},\sigma\circ i]$$

ここで, $j(\mathbb{E})$ は constant ではないので, $\mathrm{Aut}(\mathbb{E})=\{\pm1\}$. このことから上の作用は, R への群

$$(\mathrm{Aut}(E)/\{\pm1\})\times(\mathrm{Aut}(E')/\{\pm1\})$$

の free action を引き起こす.

さらに, S が coarse moduli であることから, $(\mathbb{E},\mathbb{E}')_{/R}$ は S の R-値点を与える. 従って, W 上の局所環の射

$$R_0\to R$$

を引き起こす. このとき,

命題 5.1 ([Katz-Mazur], 8.2.3) この射は同型

$$R_0\cong R^{(\mathrm{Aut}(E)/\{\pm1\})\times(\mathrm{Aut}(E')/\{\pm1\})}$$

を与える.

□

従って $R_0\to R$ は finite であり, どちらも regular local だから flat. そこで,

$$u_E:=\frac{1}{2}\sharp\mathrm{Aut}(E),\ u_{E'}:=\frac{1}{2}\sharp\mathrm{Aut}(E')$$

とおくと, R は R_0 上の階数 $u_Eu_{E'}$ の自由加群である.

この射で R に移行すると, 局所交点数は

$$\begin{aligned}(T_{m_1},T_{m_2},T_{m_3})_{[E,E']}&=\log\mathrm{lg}_W(R_0/(\varphi_{m_1},\varphi_{m_2},\varphi_{m_3}))\\ &=\log(\frac{1}{u_Eu_{E'}}\mathrm{lg}_W(R/(\varphi_{m_1},\varphi_{m_2},\varphi_{m_3})).\end{aligned}$$

ここで, 次の定理が成立する.

定理 5.2 (定理 A, ARGOS seminar の本の Ch.4, Lemma 4.1) R において φ_m は次のように分解する.

$$\varphi_m = \prod_f \varphi_{m,f}$$

ただし, 積は

$$\{f : E \to E' \mid \textit{degree}{=}m \text{ の } \textit{isogeny}\}/\pm 1$$

を走り, $\varphi_{m,f}$ は次の性質を満たすある R の元.

「R のイデアル $(\varphi_{m,f})$ は, f が R/I 上の *isogeny* $\mathbb{E}\otimes R/I \to \mathbb{E}'\otimes R/I$ に *lift* するようなイデアル I の中で最小のもの.」 *(こういう最小の I を f の* **lifting locus** *という)*

□

これを使うと, 局所交点数は次のように分解することが分かる.

$$(T_{m_1}, T_{m_2}, T_{m_3})_{[E,E']} = \log \sum_{(f_1,f_2,f_3)} \frac{1}{u_E u_{E'}} \operatorname{lg}_W(R/I),$$

但し (f_1, f_2, f_3) は集合

$$\prod_{i=1}^{3} (\{f : E \to E' : \text{degree } m_i \text{ の isogeny}\}/\{\pm 1\})$$

を走り, I は $f_i : E \to E'$ $(i = 1, 2, 3)$ が全て $\mathbb{E}\otimes_R R/J \to \mathbb{E}'\otimes_R R/J$ に lift するようなイデアル J のうちの最小のもの.

そこで,

$$\alpha_p(f_1, f_2, f_3) := \operatorname{lg}_W(R/I)$$

とおく. また, $\mathbb{Z}$ 上の quadratic space Q を,

$$Q(x_1, x_2, x_3) := \deg(x_1 f_1 + x_2 f_2 + x_3 f_3)$$

で定める. これは quadratic space $(\operatorname{Hom}(E, E'), \deg)$ の sub-quadratic space で, 主定理 (i) から, (三つの divisor が proper に交わっているという仮定により) Q は positive definite な ternary quadratic space になることがわかる.

このとき,

定理 5.3 (定理 B, ARGOS seminar の本の Ch.13, Theorem 1.1) *(i)* $\alpha_p(f_1, f_2, f_3)$ は $Q_p := Q\otimes\mathbb{Z}_p$ の同型類にしかよらない. そこで, これを $\alpha_p(Q)$ と書く.

(ii) Q_p の *Gross-Keating invariant* を (a_1, a_2, a_3) とすると, $\alpha_p(Q)$ は次の式で与えられる.

- $a_1 \equiv a_2 (2)$ のとき,

$$\alpha_p(Q) = \sum_{i=0}^{a_1-1} (i+1)(a_1+a_2+a_3-3i)p^i + \sum_{i=a_1}^{\frac{a_1+a_2-2}{2}} (a_1+1)(2a_1+a_2+a_3-4i)p^i + \frac{a_1+1}{2}(a_3-a_2+1)p^{\frac{a_1+a_2}{2}}$$

- $a_1 \not\equiv a_2 (2)$ のとき,

$$\alpha_p(Q) = \sum_{i=0}^{a_1-1}(i+1)(a_1+a_2+a_3-3i)p^i + \sum_{i=a_1}^{\frac{a_1+a_2-1}{2}}(a_1+1)(2a_1+a_2+a_3-4i)p^i$$

□

そこで, さっきの和を Q の言葉で書き表すことを考える. $\sum_{(f_1,f_2,f_3)}$ の中に同じ Q が出てくる回数は,

$$\begin{aligned}&\sharp\{Q \to (\mathrm{Hom}(E,E'), \deg) : \text{isometry}\}/\{\pm 1\}\times\{\pm 1\}\times\{\pm 1\}\\ &= \frac{1}{8}\mathrm{R}_{\mathrm{Hom}(E,E')}(Q).\end{aligned}$$

但し $\mathrm{R}_{\mathrm{Hom}(E,E')}(Q)$ は Q の $\mathrm{Hom}(E,E')$ における representation number.

ここで, E, E' は $\bar{\mathbb{F}}_p$ 上の supersingular elliptic curve だったので,

$$\begin{aligned}&\mathrm{Hom}(E,E')\otimes\mathbb{Q}_p \cong D_p := (\mathbb{Q}_p \text{ 上の division quaternion algebra})\\ &\mathrm{Hom}(E,E')\otimes\mathbb{Q}_l \cong \mathrm{M}_2(\mathbb{Q}_l)\ (l \neq p)\end{aligned}$$

が成立. したがって, $Q\otimes\mathbb{Q}_p$ が anisotropic かつ $Q\otimes\mathbb{Q}_l$ が isotropic でないと, $\mathrm{R}_{\mathrm{Hom}(E,E')}(Q) = 0$ となる. さらに, Q の定義から Q の対角成分 $\mathrm{diag}(Q)$ は (m_1, m_2, m_3) と一致していなければならない. つまり

$$(T_{m_1}, T_{m_2}, T_{m_3}) = \sum_{p<4m_1m_2m_3}\log(p)\cdot\frac{1}{8}\sum_{[E,E']_{/\bar{\mathbb{F}}_p}:\mathrm{ss.}}\sum_{Q}\alpha_p(Q)\frac{\mathrm{R}_{\mathrm{Hom}(E,E')}(Q)}{u_E u_{E'}}.$$

但し $\sum_Q$ は,

$\mathbb{Z}$ 上の positive definite な ternary quadratic space Q で,
$Q\otimes\mathbb{Q}_p$ が anisotropic, $l \neq p$ に対しては $Q\otimes\mathbb{Q}_l$ が isotropic かつ,
$\mathrm{diag}(Q) = (m_1, m_2, m_3)$ なるもの

をわたる和.

従って, 次の定理から主定理の (iii) が従う.

定理 5.4 (定理 C, ARGOS seminar の本の Ch.5, Corollary 4.4) 上のような Q に対し,

$$\sum_{[E,E']_{/\bar{\mathbb{F}}_p}:ss.}\frac{\mathrm{R}_{\mathrm{Hom}(E,E')}(Q)}{u_E u_{E'}} = 4\prod_{l|\Delta(Q), l\neq p}\beta_l(Q).$$

□

注 5.5 定理 A, B, C の証明の大筋について延べる.

- 定理 A は難しくない. 1-次元 formal group の deformation theory の帰結 (E の原点における formal completion $\hat{E}$ が height 2 の formal group だから, $\dim_{\bar{\mathbb{F}}_p}(\mathrm{H}^2(\hat{E}, \bar{\mathbb{F}}_p)) = 1$ となる. このことから lifting locus が divisor であることが従う).

- 定理 C は geometric な部分であり, classical. D を $\{p,\infty\}$ で分岐する $\mathbb{Q}$ 上の quaternion algebra, $\mathcal{O}_D$ を適当な maximal order とすると, 全単射

$$\begin{aligned}(\bar{\mathbb{F}}_p \text{ 上の supersingular elliptic curve の同型類}) &\cong D^\times \backslash (D\otimes\mathbb{A}_f)^\times/(\mathcal{O}_D\otimes\hat{\mathbb{Z}})^\times \\ &\cong (\mathcal{O}_D \text{ の右イデアル類群})\end{aligned}$$

が存在する. また, $\mathcal{O}_D$ の, D の $\mathbb{Z}$-lattice としての $\mathrm{SO}(D)(\mathbb{A}_f)$-orbit (i.e. $\mathcal{O}_D$ の **genus**) を考えると, その $\mathrm{SO}(D)(\mathbb{Q})$-同値類 (i.e. $\mathcal{O}_D$ の **proper class**) は全て $\bar{\mathbb{F}}_p$ 上の supersingular elliptic curve E, E' に対する $\mathrm{Hom}(E,E')$ で代表される (これは D の $\mathbb{Z}$-lattice と見なせる). さらにこのとき, $u_E u_{E'}$ と $\sharp\mathrm{SO}(\mathrm{Hom}(E,E'))$ はほぼ等しい. これらのことから, 次の等式を証明できる.

$$\sum_{[E,E']_{/\bar{\mathbb{F}}_p}:\mathrm{ss.}} \frac{\mathrm{R}_{\mathrm{Hom}(E,E')}(Q)}{u_E u_{E'}} = 4\sum_{[L]} \frac{\mathrm{R}_L(Q)}{\sharp\mathrm{SO}(L)},$$

但し $[L]$ は上のような各 $\mathrm{SO}(D)(\mathbb{Q})$-同値類を動く. 右辺の和は, quadratic space の lattice の representation number に関する Minkowski-Siegel の公式から, local density の積で書ける.

- 定理 B が arithmetic な部分であり, 一番難しい. 結局 R 上のこのような局所交点数を求めることは, 次のような問題に帰着される.

  - $\mathrm{Frac}(W)$ の有限次拡大 M' の整数環 A' 上に, $G=\hat{E}$ の formal group としての lift F' で, $\mathrm{End}_{A'}(F')$ が $\mathbb{Q}_p$ の二次拡大 L の order $\mathcal{O}_s$ であるようなもの, が与えられたとする. π' を A' の素元, $A'_n := A'/(\pi')^{n+1}$ とおく. このとき, $f\in\mathrm{End}_{\bar{\mathbb{F}}_p}(G)=\mathcal{O}_{D_p}$ が isogeny $F'\otimes A'_n \to F'\otimes A'_n$ に lift するような最大の n を求めること.

  Π を $\mathcal{O}_{D_p}$ の素元とし, 次のような filtration を考える.

$$\mathrm{End}_{A'}(F')=\mathcal{O}_s\subseteq\cdots\subseteq\mathcal{O}_s+\Pi^l\mathcal{O}_{D_p}\subseteq\mathcal{O}_s+\Pi^{l-1}\mathcal{O}_{D_p}\subseteq\cdots\subseteq\mathcal{O}_{D_p}=\mathrm{End}_{\bar{\mathbb{F}}_p}(G)$$

  Keating の lifting theorem (Compositio Math. **67** (1988) 211-239, ARGOS seminar の本の Ch. 11, Theorem 2.1) によると, $f\in\mathrm{End}_{\bar{\mathbb{F}}_p}(G)$ がこの filtration のどの段階に入っているかで, f がどの A'_n まで lift できるかが決まる. 属している filtration の位置は, 考えている Q の Gross-Keating invariant で表すことができるため, 定理 B が従う.

6 Siegel Eisenstein 級数のフーリエ係数との関係

weight 2 の **Siegel Eisenstein 級数**

$$E(\tau,s) := \det(y)^{\frac{s}{2}}\sum_{(c,d)}\det(c\tau+d)^{-2}|\det(c\tau+d)|^{-s}$$

を考える. 但し,

$$\tau\in\mathfrak{h}_3 := \{\tau=x+iy\in\mathrm{Sym}_3(\mathbb{C})\mid x,y\in\mathrm{M}_3(\mathbb{R}),\ y \text{ は positive definite}\}$$

を Siegel 上半空間の元, (c,d) は

$$\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\}\backslash\mathrm{Sp}_6(\mathbb{Z}) = \{g\in\mathrm{GL}_6(\mathbb{Z})\mid g\begin{pmatrix} 0 & 1_3 \\ -1_3 & 0\end{pmatrix}{}^t g = \begin{pmatrix} 0 & 1_3 \\ -1_3 & 0\end{pmatrix}\}$$

の代表元 $\begin{pmatrix} 1_3 & 0 \\ c & d \end{pmatrix}$ を動くものとする．$E(\tau, s)$ は **Fourier 展開**

$$E(\tau, s) = \sum_{T \in \mathrm{Sym}_3^\vee(\mathbb{Z})} c(T, y, s) q^T,$$

但し $\tau = x + iy \in \mathfrak{h}_3$, $q^T := \exp(2\pi i \mathrm{Tr}(T\tau)$, を持つ.

定理 6.1 (Kudla, ARGOS seminar の本の Ch.16, Theorem 2.2, Corollary 2.3) ある定数 $\kappa \in \mathbb{R}$ が存在して, 主定理 (i) の条件を満たす m_1, m_2, m_3 に対し,

$$(T_{m_1}, T_{m_2}, T_{m_3}) = \kappa \sum_T c'(T)$$

が成立．ここで, $\sum_T$ は $T \in \mathrm{Sym}_3^\vee(\mathbb{Z})$ で, *positive definite* かつ対角成分$=(m_1, m_2, m_3)$ であるものの全体を動き,

$$c'(T) = (\frac{\partial}{\partial s} c(T, y, s))|_{s=0}$$

で, これは y によらない.

証明の背景. H を $\mathbb{Z}_l$ 上の hyperbolic plane とする．つまり, $\mathbb{Z}_l$ 上の binary quadratic space で, $Q(x, y) = xy$ で定まるもの．このとき, $H^2 \cong (\mathrm{M}_2(\mathbb{Z}_l), \det)$ となる.

$\mathbb{Z}_l$ 上の ternary quadratic space Q_l に対し, 多項式 $f_{Q_l}(T) \in \mathbb{Q}[T]$ で,

$$f_{Q_l}(l^{-r}) = \alpha_l(Q_l, H^{2+r})$$

を満たすものの存在が知られている．さらに,

$$\tilde{F}_{Q_l}(T) := \frac{f_{Q_l}(T)}{(1 - l^{-2}T)(1 - l^{-2}X^2)}$$

とおく．定義から,

$$\beta_l(Q) = \tilde{F}_{Q_l}(1)$$

である．ここで, $\tilde{F}_{Q_l}(T)$ は Q の不変量を使って具体的に計算することが出来る (Katsurada, Amer. J. Math. **121** (1999) 415-452).

この結果を使って, $\mathbb{Z}_p$ 上の regular ternary quadratic space (M, Q_p) に対し

$$-(\frac{d}{dT} \tilde{F}_{Q_p}(T))|_{T=1}$$

を計算すると, これが定理 B で求めた $\alpha_p(Q_p)$ と一致する (!!) ことが確かめられる．つまり

$$\alpha_p(Q_p) = -(\frac{d}{dT} \tilde{F}_{Q_p}(T))|_{T=1}.$$

従って問題の交点数は, 各素数 l に対する $\tilde{F}_{Q_l}(T)$ たちの $T = 1$ での値と微分の値で書くことが出来る．このような $\tilde{F}_{Q_l}(T)$ が Siegel Eisenstein 級数のフーリエ係数と結び付くことは前から知られていたので, 右辺と左辺が結び付く.

7 Theorem D の Statement: local density の計算

定理 7.1 *(i) Q: $\mathbb{Z}_p$ 上の regular, anisotropic ternary 二次形式, D_p: $\mathbb{Q}_p$ 上の quaternion division algebra,* Nrd を *reduced norm* とすると,

$$\alpha_p(Q, (\mathcal{O}_{D_p}, \mathrm{Nrd})) = 2(p+1)(1+\frac{1}{p})$$

(ii) T: $\mathbb{Z}_p$ 上の regular, isotropic ternary 二次形式, (a_1, a_2, a_3): T の Gross-Keating invariant とすると,

- $a_1 \not\equiv a_2 \bmod 2$ なら,

$$\beta_p(T) = 2(\sum_{i=0}^{a_1-1}(i+1)p^i + \sum_{i=a_1}^{\frac{1}{2}(a_1+a_2-1)}(a_1+1)p^i).$$

- $a_1 \equiv a_2 \bmod 2$ のときは, $\tilde{\xi}$ を次のように定める.
  - $p \neq 2$ の場合は, T の *orthogonal basis* $\{\psi_1, \psi_2, \psi_3\}$ で $T(\psi_i) = u_i p^{a_i}$ なるものを取るとき, $\tilde{\xi} := (\frac{-u_1u_2}{p})$.
  - $p = 2$ の場合は, 上のような T の各同型類ごとに適当に $\tilde{\xi} \in \{\pm 1\}$ を定義する.

  すると,

  - $\tilde{\xi} = 1$ のとき,

$$\beta_p(T) = 2(\sum_{i=0}^{a_1-1}(i+1)p^i + \sum_{i=a_1}^{\frac{1}{2}(a_1+a_2-2)}(a_1+1)p^i) + (a_1+1)(a_3-a_2+1)p^{\frac{a_1+a_2}{2}}.$$

  - $\tilde{\xi} = -1$ のとき,

$$\beta_p(T) = 2(\sum_{i=0}^{a_1-1}(i+1)p^i + \sum_{i=a_1}^{\frac{1}{2}(a_1+a_2-2)}(a_1+1)p^i) + (a_1+1)p^{\frac{a_1+a_2}{2}}.$$

8 Hilbert symbol

定義 8.1 $a, b \in \mathbb{Q}_p^\times$ に対し, $a = up^m, b = vp^n$ $(u, v \in \mathbb{Z}_p^\times)$ と書くとき, Hilbert symbol $(a,b)_p$ を次のように定める.

- $p \neq 2$ のとき.

$$(a,b)_p := (-1)^{mn\cdot\frac{p-1}{2}}(\frac{u}{p})^n(\frac{v}{p})^m,$$

  但し $(\frac{u}{p})$ は平方剰余記号 (とくに $a, b \in \mathbb{Z}_p^\times$ なら $(a,b)_p = 1$ に注意).

- $p = 2$ のとき.

$$(a,b)_2 := (-1)^{\epsilon(u)\epsilon(v)+n\omega(u)+m\omega(v)},$$

  但し $\epsilon(u) := \frac{u-1}{2}$, $\omega(u) := \frac{u^2-1}{8}$.

命題 8.2 $Q(X_1f_1+\cdots+X_nf_n)=a_1X_1^2+\cdots+a_nX_n^2$ を $\mathbb{Q}_p$ 上の *regular quadratic space* とし,

$$d=a_1\cdots a_n,$$

$$\epsilon_p=\prod_{i>j}(a_i,a_j)_p$$

とおく. このとき, Q が *isotropic* であるための必要十分条件は, 以下のいずれかが成立すること.

(i) $n=2$ かつ $-d\in(\mathbb{Q}_p^\times)^2$

(ii) $n=3$ かつ $(-1,-d)_p=\epsilon_p$

(iii) $n=4$ かつ 「$d\notin(\mathbb{Q}_p^\times)^2$ または $\epsilon_p=(-1,-1)_p$」

(iv) $n\geq 5$