数理解析研究所講究録
第 843 巻 1993 年 127-129

On representation of positive definite quadratic forms with congruence and primitivity conditions

名大 北岡良之 (YOSHIYUKI KITAOKA)

$S^{(m)}, T^{(n)}$ を各々 m, n 次の整数係数正値対称行列とし以下の命題 (L),(G) を考えます。

(L) : $S[X_p] := {}^tX_pSX_p = T$ となる $X_p \in M_{m,n}(\mathbf{Z}_p)$ が全ての素数 p に対して存在する。

(G) : $S[X] = T$ となる $X \in M_{m,n}(\mathbf{Z})$ が存在する。

この時問題は命題 (L) から命題 (G) が従うかどうかというものである。

順序として、$\mathbf{Z}$ の代わりに $\mathbf{Q}$ で考えた場合には肯定的でありそれが Minkowski-Hasse の定理と呼ばれるものであり、この定理に因んで、ある命題が局所的に成り立てば大局的に成り立つとき Minkowski-Hasse の原理が成り立つといわれる。

次に $\mathbf{Z}$ の場合でも S が正定値ではない場合、即ち S が不定値の場合には $m \geq n+3$ の場合にはやはり肯定的である。

さて、問題としている正定値の場合に戻る。次の定理が出発点である。

定理 1 . (1) 以下の条件を満たす S にのみ依る定数 $C(S)$ が存在する。

もし $min(T) := min_{0 \neq x \in \mathbf{Z}^n} T[x] > C(S)$ かつ $m \geq 2n+3$ ならば (L) から (G) が従う。

(2) P を $2det(S)$ で割れる自然数とすると、以下の条件を満たす S, P に依る定数 $C(S,P)$ が存在する。

もし $min(T) := min_{0 \neq x \in \mathbf{Z}^n} T[x] > C(S,P)$ かつ $m \geq 3n+3$ ならば (L) から (G) が従い、更に (G) の解 X を P を割る素数 p に対し $X \equiv X_p \bmod P\mathbf{Z}_p$ であり、且つ X の単因子の素因子は P を割るように取れる。

ここですぐ問題となるのは、(1),(2) における条件 $m \geq 2n+3$ や $m \geq 3n+3$ が最良かどうかである。(1) の $m \geq 2n+3$ については $n=1$ の時には最良であることは判っているが $n \geq 2$ の時には最良ではないと思うが余りよく判っていない。かなり難しそうである。
次数に関する条件は congruence condition や primitivity condition を付けても変わらないと思われる。今回の報告の主な目的は (2) の 条件 $m \geq 3n+3$ の改良である。

定理 2 (M.JÖCHNER,Y.KITAOKA). P を $2det(S)$ で割れる自然数, e を自然数、そして q を P を割らない素数とする。

(1) 以下の条件を満たす S, P, q にのみ依る定数 $C_1(S,P,q), C_2(S,P,q)$ が存在する。

もし $min(T) := min_{0 \neq x \in \mathbf{Z}^n} T[x] > C_1(S,P,q)$ かつ $m \geq 2n+3$ ならば (L) から (G) が従い、更に (G) の解 X を P を割る素数 p に対し $X \equiv X_p \bmod P\mathbf{Z}_p$ であり、X の単因子の素因子は qP を割り, 且つ $ord_q(X$ の単因子$) \leq C_2(S,P,q)$ となるように取れる。

(2) 以下の条件を満たす S, P, q に依る定数 $C_3(S,P,q)$ が存在する。

もし $min(T) := min_{0 \neq x \in \mathbf{Z}^n} T[x] > C_3(S,P,q)$ 、 $ord_q(det(T)) \leq e$ かつ $m \geq 2n+3$ ならば (L) から (G) が従い、更に (G) の解 X を P を割る素数 p に対し $X \equiv X_p \bmod P\mathbf{Z}_p$ であり、且つ X の単因子の素因子は P を割るように取れる。

従ってもし合同条件のみを考えるならば、条件 $m \geq 3n+3$ は $m \geq 2n+3$ にまで改良されたことになる。証明については Journ. of Number Theory に出る予定なので興味ある方はそちらをご覧いただくことにしてここでは、上で、次数に関する条件は congruence condition や primitivity condition を付けても変わらないと思われると述べた理由を保形形式の立場から説明したい。

$$r(S,T) := \sharp\{X \in M_{m,n}(\mathbf{Z}) | S[X] = T\}$$
$$r(S,T,\{X_p\}_P) := \sharp\{X \in M_{m,n}(\mathbf{Z}) | S[X] = T, X \equiv X_p \bmod P\mathbf{Z}_p\}$$

と置く。$r(S,T)$ の生成関数として

$$\begin{aligned}\theta(z^{(n)},S) :&= \sum_{G \in M_{m,n}(\mathbf{Z})} e(tr(S[G]z)) \\ &= \sum r(S,T)e(tr(Tz))\end{aligned}$$

を考える。ここで z は Siegel の上半空間 $H_n := \{z \in M_n(\mathbf{C}) | z = {}^t z, Im(z) > 0\}$ の点である。この時 $\theta(z^{(n)},S)$ はいわゆる重さ $m/2$、次数 n の保形形式である。従ってそれを Eisenstein series と各 cusp での Fourier 展開の定数項が零となる保形形式の和と表し、各々の Fourier 係数を評価することによって $m \geq 4n+4$ ならば

$$r(S,T) = C(S,T)|T|^{(m-n-1)/2} + O((min(T)^{1-m/4}|T|^{(m-n-1)/2})$$

を得る。ここで、条件 (L) が成立すれば $m \geq 2n+3$ の時 $C(S,T) > C(S)$ と成る T に依らない正の定数 $C(S)$ が存在する。特に $m \geq 4n+4$ なら上の式は $r(S,T)$ の漸近式を与えている。さて合同条件のついた時には

$$\begin{aligned}\theta(z^{(n)},S,\{X_p\}_P) :&= \sum_{\substack{G \in M_{m,n}(\mathbf{Z}) \\ G \equiv X_p \, mod \, P\mathbf{Z}_p}} e(tr(S[G]z)) \\ &= \sum r(S,T,\{X_p\}_P)e(tr(Tz))\end{aligned}$$

を考える。これもまた重さ $m/2$、次数 n の保形形式となる。従ってまた $m \geq 4n+4$ なら上の式は $r(S,T)$ の漸近式を与えている。このことから問題は Eisenstein series の Fourier 係数の下からの評価と、各 cusp での Fourier 展開の定数項が零となる保型形式の Fourier 係数の上からの評価であり congruence condition をつけても生成関数 θ の level が上がるだけのことだから $m \geq 2n+3$ において $r(S,T)$ の漸近式が存在するなら $r(S,T,\{X_p\}_P)$ に対しても漸近式が存在することは当然と思われる。

次に primitivity について見てみよう。簡単のため合同条件は外すことにする。

$$r_{pr}(S,T) := \sharp\{X \in M_{m,n} | S[X] = T, X : \text{primitive}\}$$

と置くとこれは残念ながらこれは一般には modular form の Fourier 係数とはならない。しかし

$$r(S,T)=\sum_{\substack{A\in GL_n(\mathbf{Z})\backslash M_n(\mathbf{Z})\\ det(A)\neq 0}} r_{pr}(S,T[A^{-1}])$$

という関係式がある。これを Möbius 変換を用いて逆に解いて

$$r_{pr}(S,T)=\sum_{\substack{A\in GL_n(\mathbf{Z})\backslash M_n(\mathbf{Z})\\ det(A)\neq 0}} \pi(A)r(S,T[A^{-1}])$$

を得る。ここで $\mathbf{Z}_p^n/\mathbf{Z}_p^nA$ を $\mathbf{Z}_p$ 上の加群と見て $\mathbf{Z}_p/p\mathbf{Z}_p$ が 現れる個数を h_p とするとき $\pi(A):=\prod_p(-1)^{h_p}p^{h_p(h_p-1)/2}$ と置いた。但し、p は全ての素数を動くものとする。従って、$r(S,T)$ について“良い”漸近式があれば $r_{pr}(S,T)$ について漸近式がある。例えば、$m\geq 2n+2$ ならある $\epsilon>0$ に対して error term $=O((min(T))^{-\epsilon}det(T)^{(m-n-1)/2})$ であれば良い。　しかしこの error term の評価は $m\leq 4n+3$ の時には証明がかなり難しくなるように(私には)思われる。そうでなければ 定理 2 で例外的な素数の存在を許すことはないのではないかと思われる。出来ないことの言い訳にしか過ぎないが。

定理 2 の (2) の条件 $ord_q(det(T))\leq e$ は $n=1,2$ の時は省ける。これは代数的にも解析的にも証明できる。$n=1$ の時は“通常の方法”でといってよいと思うが、$n=2$ の時は技巧的であり $n\geq 3$ に拡張するのは容易ではない様に思われる。