

On the numbers of lattice points in the square  
 $|x| + |y| \leq u$  satisfying  $x + py \equiv 0 \pmod{g}$

阪大 理 山本芳彦

今  $g$  を与えられた正整数とし,  $p$  は  $g$  と互に素な整数とする. 正整数  $u$  に対して

$$(1) \quad \begin{cases} |x| + |y| \leq u \\ x + py \equiv 0 \pmod{g} \end{cases}$$

をみたす整数の組  $(x, y) \in \mathbb{Z}^2$  の個数を  $a(u; p, g)$  と表わす.  $p'$  をもう一つの整数として, 以後いつも  $(p, g) = (p', g) = 1$  と仮定する. もし  $p, p'$  が合同式  $p \equiv \pm p' \pmod{g}$  または  $pp' \equiv \pm 1 \pmod{g}$  の一つをみたすならば, 明らかに, すべての正整数  $u$  に対して,  $a(u; p, g) = a(u; p', g)$  となる. ここではこの逆も成立することを示す:

定理1. すべての正整数  $u$  に対して,  $a(u; p, g) = a(u; p', g)$  ならば,  $p \equiv \pm p' \pmod{g}$  または  $pp' \equiv \pm 1 \pmod{g}$  である.

この問題は微分幾何のある問題と関係してりて、その一つの解答を与えるものである: いま, 位数  $g$  の巡回群を基本群にもつ 3次元レンズ空間を考える. このとき, "そのリーマン多様体としての構造は Laplacian のスペクトルにより特徴付けられるか?" という問題が上記の整数論的問題に還元されるのである.  $g$  が特別の場合,  $g = l^m$  または  $g = 2l^m$  ( $l$  は素数), には Ikeda-Yamamoto [1] により肯定的に解かれてゐるが, 定理 1 はこれが一般に肯定的であることを示している (c.f. [1], [2]).

整数の組  $(x, y)$  が (1) をみたすとき, 明らかに  $(-x, -y)$  も (1) をみたすことより,

$$(2) \quad \begin{cases} x \geq 0, & x + |y| = u \\ x + py \equiv 0 \pmod{g} \end{cases}$$

をみたす  $(x, y)$  の個数を  $b(u; p, g)$  と表わすとき, 定理 1 は次の定理と同値である.

定理 2. すべての正整数  $u$  に対して,  $b(u; p, g) = b(u; p', g)$  ならば,  $p \equiv \pm p' \pmod{g}$  または  $pp' \equiv \pm 1 \pmod{g}$  である.

いま,  $\zeta = e^{2\pi i/g}$  とし,

$$F_j(x) = \frac{1}{(1-\zeta^j x)(1-\zeta^{pj} x)} + \frac{1}{(1-\zeta^j x)(1-\zeta^{-pj} x)}$$

$$G(X) = \sum_{j=0}^{g-1} F_j(X)$$

と定めると、 $G(X)$  は  $X$  の有理関数であって、 $b(u; p, g)$  の母関数となる、即ち  $X=0$  で

$$G(X) = 2g + g \sum_{u=1}^{\infty} X^{gu} + g \sum_{u=1}^{\infty} b(u; p, g) X^u$$

と展開される。  $p$  の代りに  $p'$  を用いて  $G'(X)$  を同様に定義すれば、定理 2 は次の定理と同値になる。

定理 3.  $G(X) = G'(X)$  ならば  $p \equiv \pm p' \pmod{g}$  または  $pp' \equiv \pm 1 \pmod{g}$  である。

以下では定理 3 を証明する。

### 1. $G(X)$ の極と留数

$G(X)$  は  $X = \zeta^k$  ( $k=0, 1, \dots, g-1$ ) での  $\pm$  高々 2 位の極をもつ。特に  $\zeta^k$  が  $\pm$  度 2 位の極となる必要十分条件は

$$k \equiv 0 \pmod{\frac{g}{(p-1, g)}} \text{ または } k \equiv 0 \pmod{\frac{g}{(p+1, g)}}$$

である。また 1 位の極ではその留数が

$$\begin{aligned} (3) \quad & \frac{1}{1 - \zeta^{-k(p-1)}} + \frac{1}{1 - \zeta^{-k(s-1)}} + \frac{1}{1 - \zeta^{k(p+1)}} + \frac{1}{1 - \zeta^{k(s+1)}} \\ & = 2 - \frac{1}{2} I_k \end{aligned}$$

$$I_k = \cot \frac{(p-1)k\pi}{f} + \cot \frac{(s-1)k\pi}{f} - \cot \frac{(p+1)k\pi}{f} - \cot \frac{(s+1)k\pi}{f}$$

( $\epsilon = \pm 1$   $s$  は  $ps \equiv 1 \pmod{f}$  を満たす整数) とする。  
 従って,  $G(X) = G'(X)$  ならば  $G(X)$  と  $G'(X)$  は同じ極と  
 同じ留数を持つことより, 必要ならば  $p$  と  $-p$  を交換すること  
 によつて,

$$(4) \quad \begin{cases} (p-1, f) = (p'-1, f) = \epsilon u_1 \\ (p+1, f) = (p'+1, f) = \epsilon u_2 \\ f = \epsilon u_1 u_2 r, \quad (u_1, u_2) = 1 \\ \epsilon = (p-1, p+1, f) = 1 \text{ or } 2 \end{cases}$$

よつ

(5)  $I_k = I'_k$  ( $k \not\equiv 0 \pmod{u_1 r}$  かつ  $k \not\equiv 0 \pmod{u_2 r}$ )  
 を得る ( $\epsilon = \pm 1$   $I'_k$  は  $p$  の代りに  $p'$  を用いて  $I_k$  と同様に  
 定義したものの).  $s'$  を  $p's' \equiv 1 \pmod{f}$  とする整数と  
 し,  $(p \pm 1, f) = (s \pm 1, f)$ ,  $(p' \pm 1, f) = (s' \pm 1, f)$   
 とすることより

$$\begin{cases} p-1 = \epsilon u_1 a & p'-1 = \epsilon u_1 a' \\ s-1 = \epsilon u_1 b & s'-1 = \epsilon u_1 b' \\ p+1 = \epsilon u_2 c & p'+1 = \epsilon u_2 c' \\ s+1 = \epsilon u_2 d & s'+1 = \epsilon u_2 d' \end{cases}$$

とおくと

$$I_k = \cot \frac{ak\pi}{u_2 r} + \cot \frac{bk\pi}{u_2 r} - \cot \frac{ck\pi}{u_1 r} - \cot \frac{dk\pi}{u_1 r}$$

$$I'_k = \cot \frac{a'k\pi}{u_2 r} + \cot \frac{b'k\pi}{u_2 r} - \cot \frac{c'k\pi}{u_1 r} - \cot \frac{d'k\pi}{u_1 r}$$

とある。こゝで次の補題が重要である。

補題 (Chowla, Baker-Birch-Wirsing)  $\frac{1}{2}\varphi(r)$ 個の値  
 $\cot \frac{k\pi}{r}$  ( $0 < k < r/2$  かつ  $(k, r) = 1$ )

は有理数体  $\mathbb{Q}$  上一次独立である。

## 2. 定理の証明

定理3は次の場合に証明すれば十分であることがわかる。

(I)  $g = \text{odd or } 2 \parallel g$ ;  $u_1 = u_2 = 1$ .

(II) (i)  $g = \text{odd or } 2 \parallel g$ ;  $u_1 \geq 3$ .

(ii)  $4 \parallel g$ ;  $u_1 \geq 3$ .

(iii)  $8 \parallel g$ ;  $u_1 = \text{even}$ .

(III)  $4 \parallel g$ ;  $u_1 = 2, u_2 = 1$ .

Case (I): (5)において  $k=1$  とすれば、補題より容易に

$$p \equiv \pm p' \pmod{g} \quad \text{または} \quad p \equiv \pm s' \pmod{g} \quad \text{を得る。}$$

Case (II):  $k$  を (a)  $k \equiv -1 \pmod{u_2 r}$ , (b)  $(k, g) = 1$ ,

(c)  $l \mid u_1$  かつ  $l^e \parallel u_1 r$  ( $l$  は奇素数) に対して  $k \not\equiv -1 \pmod{l}$

(d) (ciii) の場合のみ)  $2^f \parallel u_1 r$  として  $k \not\equiv -1 \pmod{2^f}$ , を

みたすように選んで,  $I_k + I_l = I'_k + I'_l$  とする

ことより

$$\begin{aligned}
 (6) \quad & \cot \frac{c\pi}{u_{ir}} + \cot \frac{d\pi}{u_{ir}} + \cot \frac{ck\pi}{u_{ir}} + \cot \frac{dk\pi}{u_{ir}} \\
 & = \cot \frac{c'\pi}{u_{ir}} + \cot \frac{d'\pi}{u_{ir}} + \cot \frac{c'k\pi}{u_{ir}} + \cot \frac{d'k\pi}{u_{ir}}
 \end{aligned}$$

となる. (6)に補題を適用して, 起り得る一次従属関係を適当に場合分けして,  $p \equiv p'$  または  $p \equiv s' \pmod{g}$  を得る.

Case(III): このときも (II)と同様に直接に補題を  $I_n = I'_n$  には適用がまほりか,  $I_1 + I_{r+1} = I'_1 + I'_{r+1}$  に対しては適用がまほることより (II)と同様に  $p \equiv p'$  または  $p \equiv s' \pmod{g}$  を得る.

### 3. 注意 ( $L(1, \chi) \neq 0$ を用いよ証明)

上記の証明では (I), (II), (III) のいずれにおいても補題の使用が key point にはなっている. 予めはまた, Dirichlet の  $L$ -関数において,  $L(1, \chi) \neq 0$  であることに基づいていふとよい (cf [1] [2]). しかし  $g = l$  (素数) の場合には, 円分体  $\mathbb{Q}(\zeta)$  での素 ideal の分解:

$$(l) = (\lambda)^{l-1}, \quad \lambda = 1 - \zeta$$

より,  $\mathbb{Q}(\zeta)_w$  ( $\lambda$ -進体) においての  $\frac{1}{1 - \zeta^k}$  ( $k = 1, 2, \dots, g-1$ ) の展開を考えるとより  $p \equiv \pm p' \pmod{l}$  または  $pp' \equiv \pm 1 \pmod{l}$  を直接に証明することができる (cf [2]).

## References

- [1] A. Ikeda and Y. Yamamoto: On the spectra of 3-dimensional lens spaces (to appear)
- [2] Y. Yamamoto: On the number of lattice points in the square  $|x| + |y| \leq u$  with a certain congruence condition.  
(in preparation)
- [3] A. Baker, B.J. Birch and E.A. Wirsing: On a Problem of Chowla, J. of Number Theory 5 (1973), 224-236.
- [4] S. Chowla: The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation, J. of Number Theory 2 (1970), 120-123.