

ディリクレの類数公式の組合せ論的変形
 (A Combinatorial Deformation of Dirichlet's Class Number Formula)

佐賀大学大学院工学系研究科システム生産科学専攻情報システム学大講座
 博士後期課程 3 年 三ッ廣 孝 (Takashi Mitsuhiro)

1. 序

素数判別式をもつ実 2 次体に対するディリクレの類数公式の変形については, H. Hasse[3], P. Chowla[1] や T. Ono[6] によるいくつかの結果が知られている. 私達はここでディリクレの類数公式の変形の 1 つの結果として, 組合せ論を使って次の定理を [5] に基づいて示す.

定理 1. $\varepsilon (> 1)$, h および $\chi(x)$ で素数判別式 $p \equiv 1 \pmod{4}$ をもつ実 2 次体 $\mathbb{Q}(\sqrt{p})$ の基本単数, 広義の類数およびクロネッカー記号を表すとし, さらに T で単数 ε^{2h} のトレース $\varepsilon^{2h} + \varepsilon^{-2h}$ を表すとする. そのとき

$$T = (1/p) \left(\sum_{k=0}^{(p-1)/2} a_k \right)^2 - 2$$

が成り立つ. ここで各有理整数 a_n, b_n は次の漸化式

$$\begin{aligned} a_0 &= 2, & 2na_n &= \sum_{k=0}^{n-1} \{a_k + \chi(n-k)b_k p\} \quad (1 \leq n \leq (p-1)/2), \\ b_0 &= 0, & 2nb_n &= \sum_{k=0}^{n-1} \{b_k + \chi(n-k)a_k\} \quad (1 \leq n \leq (p-1)/2) \end{aligned}$$

でそれぞれ定められるものとする.

私達は最近になって T. Ono による上の定理よりも少し強い次の結果を知った.

定理 2 ([6]). 素数 $p \equiv 1 \pmod{4}$ に対して $N = (p-1)/4$, $\omega = (1 + \sqrt{p})/2$, $\omega' = (1 - \sqrt{p})/2$ とおき,

$$\alpha_\nu = \begin{cases} \omega & \chi(\nu) = +1 \text{ のとき,} \\ \omega' & \chi(\nu) = -1 \text{ のとき,} \end{cases}$$

とする. ここで $\chi(\nu) = (\nu/p)$ はルシャンドル記号を表すとし, さらに $k = \mathbb{Q}(\sqrt{p})$ で判別式 p をもつ実 2 次体を表し, ε, h でそれぞれ k の基本単数, 広義の類数を表すとする. そのとき関係式

$$\sqrt{p}\varepsilon^h = 2 \sum_{n=0}^{N-1} d_n + d_N,$$

が成り立つ. ここで k の各整数 d_n は次の漸化式

$$d_0 = 1, \quad d_1 = \omega, \quad nd_n = \sum_{\nu=1}^n \alpha_\nu d_{n-\nu} \quad (1 \leq n \leq N)$$

で定められるものとする.

2. 組合せ論からの準備

この節で私達は後の節の準備として組合せ論からいくつかの定義と結果とを引用する ([4], [7], [8] 参照).

補題 2.1. (V, \preceq) で順序 \preceq をもつ有限束を表すとするとき, 3つの条件 (i) $x \not\preceq y$ のとき $\mu(x, y) = 0$, (ii) 任意の $x \in V$ に対して $\mu(x, x) = 1$, (iii) $x \prec y$ のとき $\sum_{x \preceq z \preceq y} \mu(x, z) = 0$ を満たす関数 $\mu: V \times V \rightarrow \mathbb{R}$ が一意的に定まる.

この関数 μ は有限束 V 上のメビウス関数と呼ばれる.

補題 2.2 (メビウスの反転公式). 有限束 (V, \preceq) 上の関数 f, g に対して

$$g(x) = \sum_{y \preceq x} f(y) \quad (\forall x \in V)$$

が成り立てば,

$$f(x) = \sum_{y \preceq x} g(y) \mu(y, x) \quad (\forall x \in V)$$

も成り立つ.

補題 2.3. 有限束 (V, \preceq) の順序 \preceq に対して, 反順序 \preceq_* を $x \preceq_* y \leftrightarrow y \preceq x$ ($x, y \in V$) で定義する. そのとき (V, \preceq_*) も有限束をなし, 各有限束 (V, \preceq) , (V, \preceq_*) 上のメビウス関数をそれぞれ μ, μ_* とするとき, $\mu_*(x, y) = \mu(y, x)$ ($\forall x, y \in V$) が成り立つ.

補題 2.4. $\langle n \rangle = \{1, 2, \dots, n\}$ とし, $\langle n \rangle$ の分割全体の集合を \mathbf{P}_n で表す. 各分割 $A = \{A_1, A_2, \dots, A_s\} \in \mathbf{P}_n$ に対して各 A_i ($1 \leq i \leq s$) を A のブロックという. そのとき $A = \{A_1, A_2, \dots, A_s\}$, $B = \{B_1, B_2, \dots, B_t\} \in \mathbf{P}_n$ に対して, 各ブロック A_i ($1 \leq i \leq s$) に対して $A_i \subseteq B_j$ なるブロック B_j が存在するとき $A \preceq B$ とし \mathbf{P}_n 上の順序 \preceq を定義すると, 順序集合 (\mathbf{P}_n, \preceq) は最大元 $\mathbf{1} = \{\{1, 2, \dots, n\}\}$, 最小元 $\mathbf{0} = \{\{1\}, \{2\}, \dots, \{n\}\}$ をもつ有限束をなす. そして (\mathbf{P}_n, \preceq) 上の順序 \preceq の反順序を \preceq_* とすれば, $(\mathbf{P}_n, \preceq_*)$ も有限束をなす.

いま上の記号のもとに以下 μ, μ_* をそれぞれ有限束 (\mathbf{P}_n, \preceq) , $(\mathbf{P}_n, \preceq_*)$ 上のメビウス関数を表すとす. また自然数 q, k ($1 \leq k \leq q$) に対して $(q)_k = q(q-1)\cdots(q-k+1)$ とおき, これを q - k 順列という. また集合 S の元の個数を一般に $|S|$ で表すとき, $\langle n \rangle$ の各分割 $A = \{A_1, A_2, \dots, A_s\}$ に対して各 c_i^A ($1 \leq i \leq n$) を $c_i^A = |\{j; |A_j| = i\}|$ で定義し, 組 $(c_1^A, c_2^A, \dots, c_n^A)$ を分割 A のタイプという. そのとき $\sum_{i=1}^n i \cdot c_i^A = n$, $c_i^A \geq 0$ ($1 \leq i \leq n$) が成り立つ. さらに分割 A のブロックの個数を $w_A = \sum_{i=1}^n c_i^A$ で定義する.

補題 2.5. 次が成り立つ:

$$\sum_{A \in \mathbf{P}_n} q^s \mu(\mathbf{0}, A) = (q)_n \quad (q \geq 1, 1 \leq n \leq q).$$

補題 2.6. $n \geq 1$ とするとき, タイプ (c_1, c_2, \dots, c_n) をもつ $\langle n \rangle$ の分割の個数は,

$$\frac{n!}{\prod_{i=1}^n \{c_i! \cdot (i!)^{c_i}\}}$$

で与えられる.

補題 2.7. 次が成り立つ:

$$\mu(\mathbf{0}, A) = \prod_{i=1}^s \{(-1)^{|A_i|-1} (|A_i|-1)!\} \quad (A = \{A_1, A_2, \dots, A_s\} \in P_n).$$

系 2.7.1. 次を得る.

$$\mu(\mathbf{0}, A) = (-1)^{n+w_A} \prod_{i=1}^n \{(i-1)!\}^{c_i^A} \quad (A = \{A_1, A_2, \dots, A_s\} \in P_n).$$

証明. 補題 2.7 および分割のタイプの定義よりわかる.

この節の最後として, 記号 \sum_n^* で条件 $\sum_{i=1}^n i \cdot c_i = n$, $c_i \geq 0$ ($1 \leq i \leq n$) を満たす組 (c_1, c_2, \dots, c_n) すべてにわたる和を表すとき, n 次対称群 S_n の巡回置換指数 $\mathcal{I}_n(x_1, \dots, x_n)$ を n 変数多項式

$$\mathcal{I}_n(x_1, x_2, \dots, x_n) = (1/n!) \sum_n^* h_{c_1 c_2 \dots c_n} x_1^{c_1} x_2^{c_2} \dots x_n^{c_n}$$

で定義する. ここで n 文字の置換 $\sigma \in S_n$ を互いに素な巡回置換 ρ_j の積として $\sigma = \rho_1 \dots \rho_s$ と表すとき,

$$h_{c_1 c_2 \dots c_n} = |\{\sigma \in S_n; |\rho_j \text{ of length } i \text{ in } \sigma| = c_i \ (1 \leq i \leq n)\}|$$

と定義する. 特に $\mathcal{I}_0 = 1$ とする.

補題 2.8. 次が成り立つ:

$$\mathcal{I}_n(x_1, x_2, \dots, x_n) = \frac{1}{n!} \sum_n^* \frac{n!}{\prod_{i=1}^n \{c_i! \cdot i^{c_i}\}} x_1^{c_1} x_2^{c_2} \dots x_n^{c_n} \quad (n \geq 1).$$

補題 2.9. 次の漸化式が成り立つ:

$$n\mathcal{I}_n(x_1, x_2, \dots, x_n) = \sum_{k=1}^n x_k \mathcal{I}_{n-k}(x_1, x_2, \dots, x_{n-k}) \quad (n \geq 1).$$

3. 有限体上の方程式の解の個数

この節では、奇素数 p に対して標数 p なる有限素体上の方程式の解の個数について考える。そこで F_p で標数 p なる有限素体を表し、その既約剰余類群を F_p^\times で表す。また F_p^\times 上で定義される 2 次の指標 $\chi(x)$ を

$$\chi(x) = \begin{cases} +1 & a^2 = x \text{ なる } a \in F_p^\times \text{ が存在するとき,} \\ -1 & \text{その他,} \end{cases}$$

で定義する。また $n \geq 1$ とし、 $a_1, a_2, \dots, a_n \in F_p^\times$ に対して F_p 上の方程式

$$a_1 x_1^2 + a_2 x_2^2 + \dots + a_n x_n^2 = 0$$

の F_p における解 $x = t_1, x = t_2, \dots, x = t_n$ 全体の集合を $S(a_1, a_2, \dots, a_n)$ で、その解の個数を $N(a_1, a_2, \dots, a_n)$ でそれぞれ表す。同様に F_p^\times における解全体の集合を $S^\times(a_1, a_2, \dots, a_n)$ で、その解の個数を $N^\times(a_1, a_2, \dots, a_n)$ で表す。さらに F_p^\times における解で条件 $t_i^2 \neq t_j^2$ ($1 \leq i < j \leq n$) を満たす解全体の集合を $DS^\times(a_1, a_2, \dots, a_n)$ で、その解の個数を $DN^\times(a_1, a_2, \dots, a_n)$ で表す。特に $DN_n^\times = DN^\times(\underbrace{1, 1, \dots, 1}_n)$ ($n \geq 1$) と表す。

ここで $[x]$ で x を越えない最大の有理整数、つまりガウス記号を表すとき $N(a_1, \dots, a_n)$ の値について次の結果が知られている。

補題 3.1 (G. Fujisaki[2]). $n \geq 1, m = [n/2]$ とする。そのとき $a_1, \dots, a_n \in F_p^\times$ に対して

$$N(a_1, \dots, a_n) = \begin{cases} p^{n-1} & n \text{ が奇数のとき,} \\ p^{n-1} + \chi(a_1 \cdots a_n) (p^m - p^{m-1}) & n \text{ が偶数のとき,} \end{cases}$$

が成り立つ。

次に $n \geq 1, 0 \leq r, v \leq n$ とするとき、

$$\begin{aligned} D_n(v) &= (1 + \sqrt{p})^{n-v} (1 - \sqrt{p})^v + (1 + \sqrt{p})^v (1 - \sqrt{p})^{n-v}, \\ K_{n,r}(v) &= s_r(\underbrace{-1, -1, \dots, -1}_v, \underbrace{1, 1, \dots, 1}_{n-v}) \end{aligned}$$

とおく。ここで $s_r(x_1, x_2, \dots, x_n)$ は n 次の基本対称式

$$s_r(x_1, x_2, \dots, x_n) = \begin{cases} 1 & (r = 0), \\ \sum_{1 \leq j_1 < j_2 < \dots < j_r \leq n} x_{j_1} x_{j_2} \cdots x_{j_r} & (1 \leq r \leq n) \end{cases}$$

を表す。さらに $a_1, a_2, \dots, a_n \in F_p^\times$ に対して $v(a_1, a_2, \dots, a_n)$ で $\chi(a_j) = -1$ なる j の個数を表すとする。

命題 3.1. $v = v(a_1, a_2, \dots, a_n)$ とおくと,

$$\sum_{k=0}^{\lfloor n/2 \rfloor} K_{n,2k}(v)p^k = \frac{1}{2}D_n(v) \quad (a_1, a_2, \dots, a_n \in \mathbf{F}_p^\times)$$

が成り立つ.

証明. $1 \leq r \leq n$ に対して

$$K_{n,r}(v) = \sum_{1 \leq j_1 < j_2 < \dots < j_r \leq n} (-1)^{v(a_{j_1}, a_{j_2}, \dots, a_{j_r})} = \sum_{j=0}^r (-1)^j \binom{n-v}{r-j} \binom{v}{j}$$

が成り立ち, 特に $r=0$ のときも成り立つ. ゆえに

$$\begin{cases} (1+x)^{n-v}(1-x)^v = \sum_{k=0}^n \sum_{j=0}^k (-1)^j \binom{n-v}{k-j} \binom{v}{j} x^k = \sum_{k=0}^n K_{n,k}(v)x^k, \\ (1+x)^v(1-x)^{n-v} = \sum_{k=0}^n K_{n,k}(v)(-x)^k = \sum_{k=0}^n (-1)^k K_{n,k}(v)x^k, \end{cases}$$

となり,

$$\frac{1}{2} \left\{ (1+x)^{n-v}(1-x)^v + (1+x)^v(1-x)^{n-v} \right\} = \sum_{k=0}^{\lfloor n/2 \rfloor} K_{n,2k}(v)x^{2k}$$

が成り立つ. 特に $x = \sqrt{p}$ として命題が成り立つ.

命題 3.2. 命題 3.1 と同じ記号のもとで,

$$\mathcal{N}^\times(a_1, a_2, \dots, a_n) = \frac{1}{p} \left\{ (p-1)^n + (-1)^n \frac{1}{2}(p-1)D_n(v) \right\}$$

を得る.

証明. $1 \leq r \leq n$ に対して集合 M_r, \overline{M}_r を

$$\begin{cases} M_r = \{(t_1, t_2, \dots, t_n) \in \mathcal{S}(a_1, a_2, \dots, a_n) \mid t_r = 0\}, \\ \overline{M}_r = \{(t_1, t_2, \dots, t_n) \in \mathcal{S}(a_1, a_2, \dots, a_n) \mid t_r \neq 0\}, \end{cases}$$

とおき, また集合 $\{1, 2, \dots, n\}$ の各部分集合 $\{j_1, j_2, \dots, j_r\}$ に対して補集合 $\{1, 2, \dots, n\} \setminus \{j_1, j_2, \dots, j_r\}$ を $\{i_1, i_2, \dots, i_{n-r}\}$ で表す. そのとき

$$|M_{j_1} \cap M_{j_2} \cap \dots \cap M_{j_r}| = \begin{cases} \mathcal{N}(a_{i_1}, a_{i_2}, \dots, a_{i_{n-r}}) & (1 \leq r < n), \\ 1 & (r = n), \end{cases}$$

であり, 特に $|\overline{M}_1 \cap \overline{M}_2 \cap \dots \cap \overline{M}_n| = \mathcal{N}^\times(a_1, a_2, \dots, a_n)$ が成り立つ. ゆえに包除原理により

$$\mathcal{N}^\times(a_1, a_2, \dots, a_n) = \sum_{r=1}^n (-1)^{n-r} \sum_{1 \leq j_1 < j_2 < \dots < j_r \leq n} \mathcal{N}(a_{j_1}, a_{j_2}, \dots, a_{j_r}) + 1$$

が成り立つ。そこで $m = \lfloor n/2 \rfloor$ とおくと $\sum_{1 \leq j_1 < j_2 < \dots < j_r \leq n} \chi(a_{j_1} a_{j_2} \dots a_{j_r}) = K_{n,r}(v)$ に注意して、

$$\begin{aligned} & \sum_{k=1}^n (-1)^{n-k} \sum_{1 \leq j_1 < j_2 < \dots < j_k \leq n} \mathcal{N}(a_{j_1}, a_{j_2}, \dots, a_{j_k} + 1) \\ &= (-1)^n \left\{ \sum_{k=0}^{n-1} (-1)^{k+1} \binom{n}{k+1} p^k + \sum_{k=1}^m K_{n,2k}(v)(p^k - p^{k-1}) + 1 \right\} \\ &= \frac{1}{p} \left\{ (p-1)^n + (-1)^n \frac{1}{2} (p-1) D_n(v) \right\} \end{aligned}$$

となり、命題が成り立つ。

さて $a_1, a_2, \dots, a_n \in \mathbf{F}_p^\times$ とし、 $\langle n \rangle$ の空でない部分集合 M に対して $\lambda_M(a_1, a_2, \dots, a_n) = \sum_{j \in M} a_j \in \mathbf{F}_p$ と定義する。

命題 3.3. $a_1, a_2, \dots, a_n \in \mathbf{F}_p^\times$ とし、

$$\lambda_M = \lambda_M(a_1, a_2, \dots, a_n) \neq 0 \quad (\phi \neq \forall M \subset \langle n \rangle)$$

が成り立つと仮定する。そのとき

$$\mathcal{N}^\times(a_1, a_2, \dots, a_n) = \sum_{A=\{A_1, A_2, \dots, A_s\} \in \mathbf{P}_n} 2^{n-s} \mathcal{DN}^\times(\lambda_{A_1}, \lambda_{A_2}, \dots, \lambda_{A_s})$$

を得る。

証明. $\langle n \rangle$ の各分割 $A = \{A_1, A_2, \dots, A_s\}$ に対して、各 $i \in A_k, j \in A_l$ に対して $t_i^2 = t_j^2 \leftrightarrow k=l$ なる $(t_1, t_2, \dots, t_n) \in \mathcal{S}^\times(a_1, a_2, \dots, a_n)$ 全体の集合を $\mathcal{S}_A^\times(a_1, a_2, \dots, a_n)$ で表す。そのとき

$$\mathcal{N}^\times(a_1, a_2, \dots, a_n) = \sum_{A \in \mathbf{P}_n} |\mathcal{S}_A^\times(a_1, a_2, \dots, a_n)|$$

が成り立ち、また各 $(t_1, t_2, \dots, t_s) \in \mathcal{DS}^\times(\lambda_{A_1}, \lambda_{A_2}, \dots, \lambda_{A_s})$ に対して

$$[t_1, t_2, \dots, t_s] = \{(\bar{t}_1, \bar{t}_2, \dots, \bar{t}_n) \in \mathbf{F}_p^n; \text{ if } i \in A_j \text{ then } \bar{t}_i = \pm t_j\}$$

と定義すると、

$$\begin{aligned} \mathcal{S}_A^\times(a_1, a_2, \dots, a_n) &= \bigcup_{(t_1, t_2, \dots, t_s) \in \mathcal{DS}^\times(\lambda_{A_1}, \lambda_{A_2}, \dots, \lambda_{A_s})} [t_1, t_2, \dots, t_s], \\ [t_1, \dots, t_s] \neq [t'_1, \dots, t'_s] &\leftrightarrow [t_1, \dots, t_s] \cap [t'_1, \dots, t'_s] = \phi, \\ [t_1, \dots, t_s] = [t'_1, \dots, t'_s] &\leftrightarrow (t_1, \dots, t_s) = (\pm t'_1, \dots, \pm t'_s) \end{aligned}$$

なので、

$$\begin{aligned} & \left| \{[t_1, t_2, \dots, t_s]; (t_1, t_2, \dots, t_s) \in \mathcal{DS}^\times(\lambda_{A_1}, \lambda_{A_2}, \dots, \lambda_{A_s})\} \right| \\ &= \frac{1}{2^s} \mathcal{DN}^\times(\lambda_{A_1}, \lambda_{A_2}, \dots, \lambda_{A_s}) \end{aligned}$$

となり、以上を組み合わせて求める命題が成り立つ。

命題 3.4. 命題 3.3 と同じ記号, 仮定のもとで, $\langle n \rangle$ の分割 $B = \{B_1, B_2, \dots, B_t\}$ に対して

$$\frac{1}{2^t} \mathcal{N}^\times(\lambda_{B_1}, \lambda_{B_2}, \dots, \lambda_{B_t}) = \sum_{\substack{A = \{A_1, A_2, \dots, A_s\} \in \mathcal{P}_n \\ A \preceq_* B}} \frac{1}{2^s} \mathcal{DN}^\times(\lambda_{A_1}, \lambda_{A_2}, \dots, \lambda_{A_s})$$

が従う。

証明. $\langle n \rangle$ の各分割 $B = \{B_1, B_2, \dots, B_t\}$ に対して $\overline{\lambda}_M = \lambda_M(\lambda_{B_1}, \lambda_{B_2}, \dots, \lambda_{B_t}) \in \mathcal{F}_p$ ($\phi \neq \forall M \subset \langle t \rangle$) とおくと, 仮定より $\overline{\lambda}_M \neq 0$ がわかるので, 命題 3.3 より

$$\mathcal{N}^\times(\lambda_{B_1}, \lambda_{B_2}, \dots, \lambda_{B_t}) = \sum_{A = \{A_1, A_2, \dots, A_s\} \in \mathcal{P}_t} 2^{t-s} \mathcal{DN}^\times(\overline{\lambda}_{A_1}, \overline{\lambda}_{A_2}, \dots, \overline{\lambda}_{A_s})$$

が成り立つ。

ここで $\langle t \rangle$ の各分割 $A = \{A_1, A_2, \dots, A_s\}$ に対して $\overline{A} = \{\overline{A}_1, \overline{A}_2, \dots, \overline{A}_s\}$, $\overline{A}_i = \bigcup_{j \in A_i} B_j$ ($1 \leq i \leq s$) とおくと, $\overline{A} \in \mathcal{P}_n$, $\overline{A} \preceq_* B$ であり, 写像 $\varphi_t: \mathcal{P}_t \ni A \mapsto \overline{A} \in \mathcal{P}_n$ は単射で $\varphi_t(\mathcal{P}_t) = \{X \in \mathcal{P}_n; X \preceq_* B\}$ がわかる. ゆえに $\overline{\lambda}_{A_i} = \lambda_{\overline{A}_i}$ に注意して, $\mathcal{DN}^\times(\overline{\lambda}_{A_1}, \overline{\lambda}_{A_2}, \dots, \overline{\lambda}_{A_s}) = \mathcal{DN}^\times(\lambda_{\overline{A}_1}, \lambda_{\overline{A}_2}, \dots, \lambda_{\overline{A}_s})$ となり, 以上より命題が成り立つ。

命題 3.5. 命題 3.3 と同じ記号, 仮定のもとで, $\langle n \rangle$ の分割 $B = \{B_1, B_2, \dots, B_t\}$ に対して

$$\mathcal{DN}^\times(\lambda_{B_1}, \lambda_{B_2}, \dots, \lambda_{B_t}) = 2^t \sum_{\substack{A = \{A_1, \dots, A_s\} \in \mathcal{P}_n \\ B \preceq A}} \frac{1}{2^s} \mathcal{N}^\times(\lambda_{A_1}, \dots, \lambda_{A_s}) \mu(B, A)$$

が成り立つ。

証明. 2つの関数 $f: \mathcal{P}_n \rightarrow \mathbb{R}$ と $g: \mathcal{P}_n \rightarrow \mathbb{R}$ を

$$\begin{cases} f(X) = (1/2^s) \mathcal{DN}^\times(\lambda_{X_1}, \lambda_{X_2}, \dots, \lambda_{X_s}) \\ g(X) = (1/2^s) \mathcal{N}^\times(\lambda_{X_1}, \lambda_{X_2}, \dots, \lambda_{X_s}) \end{cases} \quad (X = \{X_1, X_2, \dots, X_s\} \in \mathcal{P}_n),$$

で定義する. そのとき命題 3.4 より任意の $\langle n \rangle$ の分割 $X = \{X_1, X_2, \dots, X_s\}$ に対して $g(X) = \sum_{Z \preceq_* X} f(Z)$ が成り立つ. ゆえに補題 2.3 およびメビウスの反転公式より, 各 $\langle n \rangle$ の分割 $B = \{B_1, B_2, \dots, B_t\}$ に対して

$$\mathcal{DN}^\times(\lambda_{B_1}, \lambda_{B_2}, \dots, \lambda_{B_t}) = 2^t f(B) = 2^t \sum_{A \preceq_* B} g(A) \mu_*(A, B) = 2^t \sum_{B \preceq A} g(A) \mu(B, A)$$

となり, 命題が成り立つ。

さてこの節の最後として, 各 $\langle n \rangle$ の分割 $A = \{A_1, A_2, \dots, A_s\}$ に対して $v_A = v(|A_1|, |A_2|, \dots, |A_s|)$ とおき, さらに $1 \leq n \leq p-1$ に対して

$$H(n) = \sum_{A \in \mathcal{P}_n} (-1)^{w_A} (1/2^{w_A}) D_{w_A}(v_A) \mu(0, A)$$

と定義し, \mathcal{DN}_n^\times ($n \geq 1$) の値を決定する. すなわち

命題 3.6. 次を得る:

$$\mathcal{DN}_n^\times = 2^n \frac{1}{p} \left\{ \left(\frac{p-1}{2} \right)_n + \frac{1}{2}(p-1)H(n) \right\} \quad (1 \leq n \leq p-1).$$

証明. もし $a_1, a_2, \dots, a_n \in \mathbf{F}_p^\times$ に対して $\lambda_M = \lambda_M(a_1, a_2, \dots, a_n) \neq 0$ ($\phi \neq \forall M \subset \langle n \rangle$) が成り立つと仮定すると, 命題 3.5 より

$$\begin{aligned} \mathcal{DN}^\times(a_1, a_2, \dots, a_n) &= \mathcal{DN}^\times(\lambda_{\{1\}}, \lambda_{\{2\}}, \dots, \lambda_{\{n\}}) \\ &= 2^n \sum_{A=\{A_1, A_2, \dots, A_s\} \in \mathbf{P}_n} \frac{1}{2^s} \mathcal{N}^\times(\lambda_{A_1}, \lambda_{A_2}, \dots, \lambda_{A_s}) \mu(\mathbf{0}, A) \end{aligned}$$

が成り立つ. そこで特に $a_1 = a_2 = \dots = a_n = 1 \in \mathbf{F}_p^\times$ とすると $\lambda_M = \lambda_M(\underbrace{1, 1, \dots, 1}_n) = |M| \neq 0$ ($\phi \neq \forall M \subset \langle n \rangle$) なので, 命題 3.2 および補題 2.5 より

$$\begin{aligned} \mathcal{DN}_n^\times &= 2^n \sum_{A=\{A_1, A_2, \dots, A_s\} \in \mathbf{P}_n} \frac{1}{2^s} \mathcal{N}^\times(|A_1|, |A_2|, \dots, |A_s|) \mu(\mathbf{0}, A) \\ &= 2^n \frac{1}{p} \sum_{A=\{A_1, A_2, \dots, A_s\} \in \mathbf{P}_n} \frac{1}{2^s} \left\{ (p-1)^s + (-1)^s \frac{1}{2}(p-1)D_s(v_A) \right\} \mu(\mathbf{0}, A) \\ &= 2^n \frac{1}{p} \left\{ \sum_{A=\{A_1, A_2, \dots, A_s\} \in \mathbf{P}_n} \left(\frac{p-1}{2} \right)^s \mu(\mathbf{0}, A) \right. \\ &\quad \left. + \frac{1}{2}(p-1) \sum_{A=\{A_1, A_2, \dots, A_s\} \in \mathbf{P}_n} (-1)^s \frac{1}{2^s} D_s(v_A) \mu(\mathbf{0}, A) \right\} \\ &= 2^n \frac{1}{p} \left\{ \left(\frac{p-1}{2} \right)_n + \frac{1}{2}(p-1)H(n) \right\} \end{aligned}$$

が成り立つ.

4. 類数公式の組合せ論的変形

この節で私達は定理 1 の証明を行い, 例とともに定理 1 と定理 2 との関連について少し述べる. そこで $\theta = \exp(2\pi i/p)$ とおき, $\chi(x)$ で実 2 次体 $\mathbf{Q}(\sqrt{p})$ に対するクロネッカー記号を表す. ここでクロネッカー記号は, 第 3 節で定義した \mathbf{F}_p^\times 上の 2 次指標 $\chi(x)$ と同一視できることに注意する.

私達はよく知られている次のディレクレの類数公式を出発点とする.

補題 4.1 (ディレクレの類数公式). 定理 1 と同じ記号のもとで,

$$\varepsilon^{2h} = \frac{\prod_{\substack{0 < n < p \\ \chi(n) = -1}} (1 - \theta^n)}{\prod_{\substack{0 < r < p \\ \chi(r) = +1}} (1 - \theta^r)}.$$

が成り立つ.

いま

$$N(\theta) = \prod_{\substack{0 < n < p \\ \chi(n) = -1}} (1 - \theta^n), \quad R(\theta) = \prod_{\substack{0 < r < p \\ \chi(r) = +1}} (1 - \theta^r)$$

とおき, さらに T で単数 ε^{2h} のトレース $\varepsilon^{2h} + \varepsilon^{-2h}$ を表すとする.

命題 4.1. 次が成り立つ:

$$T = \frac{\{N(\theta) + R(\theta)\}^2}{p} - 2.$$

証明. $N(\theta)R(\theta) = \prod_{0 < k < p} (1 - \theta^k) = p$ に注意すると,

$$T = \varepsilon^{2h} + \varepsilon^{-2h} = \frac{N(\theta)^2 + R(\theta)^2}{N(\theta)R(\theta)} = \frac{\{N(\theta) + R(\theta)\}^2}{p} - 2$$

となり成り立つ.

さて $1 \leq m \leq (p-1)/2$ および $0 \leq s \leq p-1$ に対して, 条件 $t_1 + t_2 + \dots + t_m \equiv s \pmod{p}$, $1 \leq t_1 < t_2 < \dots < t_m \leq p-1$, $\chi(t_i) = 1$ ($1 \leq i \leq m$) を満たす組 (t_1, t_2, \dots, t_m) 全体の集合を $W_m(s)$ で, その元の個数を $S_m(s) = |W_m(s)|$ で定義する. さらに各 $0 \leq k \leq p-1$ に対して $\alpha_k = \sum_{m=1}^{\frac{p-1}{2}} (-1)^m S_m(k)$ とおく.

命題 4.2. 次が成り立つ:

$$R(\theta) = 1 + \sum_{k=0}^{p-1} \alpha_k \theta^k.$$

証明. $\chi(r) = 1$ なる r ($1 \leq r \leq p-1$) を $r_1, r_2, \dots, r_{\frac{p-1}{2}}$ とおくと, 一般に

$$\prod_{i=1}^k (1 - \theta^{r_i}) = 1 + \sum_{i=1}^k (-1)^i \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq k} \theta^{r_{j_1} + r_{j_2} + \dots + r_{j_i}}$$

が成り立つので,

$$R(\theta) = \prod_{i=1}^{\frac{p-1}{2}} (1 - \theta^{r_i}) = 1 + \sum_{i=1}^{\frac{p-1}{2}} (-1)^i \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq \frac{p-1}{2}} \theta^{r_{j_1} + r_{j_2} + \dots + r_{j_i}}$$

$$= 1 + \sum_{i=1}^{\frac{p-1}{2}} (-1)^i \sum_{k=0}^{p-1} S_i(k) \theta^k = 1 + \sum_{k=0}^{p-1} \alpha_k \theta^k.$$

となり命題が成り立つ.

命題 4.3. $\chi(i) = \chi(j)$ のとき $\alpha_i = \alpha_j$ である.

証明. 各 $1 \leq i < j \leq p-1$ に対して $u_{ij} i \equiv j \pmod{p}$ なる u_{ij} ($1 \leq u_{ij} \leq p-1$) を考えると, $\chi(i) = \chi(j)$ のとき $\chi(u_{ij}) = 1$ である. そこで各元を p を法とする代表元で考えると, $\varphi_{ij} : W_m(i) \ni (t_1, t_2, \dots, t_m) \mapsto (t_1 u_{ij}^{-1}, t_2 u_{ij}^{-1}, \dots, t_m u_{ij}^{-1}) \in W_m(j)$ で写像 $\varphi_{ij} : W_m(i) \mapsto W_m(j)$ ($1 \leq i < j \leq p-1$) を定義すると, $\chi(i) = \chi(j)$ のときすべての φ_{ij} は単射であり, $S_m(i) = |W_m(i)| = |W_m(j)| = S_m(j)$ ($1 \leq m \leq (p-1)/2$) なので, $\alpha_i = \sum_{m=1}^{\frac{p-1}{2}} (-1)^m S_m(i) = \sum_{m=1}^{\frac{p-1}{2}} (-1)^m S_m(j) = \alpha_j$ がわかる.

そこで命題 4.3 より $\chi(n) = -1$ なる n に対する共通の値 α_n を α_N で, $\chi(r) = +1$ なる r に対する共通の値 α_r を α_R で表す.

命題 4.4. 次を得る:

$$\alpha_N + \alpha_R = -\frac{2}{p-1}(1 + \alpha_0).$$

証明. 各 $1 \leq m \leq (p-1)/2$ に対して, 条件 $1 \leq t_1 < t_2 < \dots < t_m \leq p-1$, $\chi(t_i) = 1$ ($1 \leq i \leq m$) を満たす組 (t_1, t_2, \dots, t_m) 全体の集合を V_m で表すと,

$$\begin{aligned} \sum_{m=1}^{\frac{p-1}{2}} (-1)^m |V_m| &= \sum_{m=1}^{\frac{p-1}{2}} (-1)^m \left\{ S_m(0) + \sum_{\substack{0 < n < p \\ \chi(n) = -1}} S_m(n) + \sum_{\substack{0 < r < p \\ \chi(r) = +1}} S_m(r) \right\} \\ &= \sum_{m=1}^{\frac{p-1}{2}} (-1)^m S_m(0) + \sum_{\substack{0 < n < p \\ \chi(n) = -1}} \sum_{m=1}^{\frac{p-1}{2}} (-1)^m S_m(n) + \sum_{\substack{0 < r < p \\ \chi(r) = +1}} \sum_{m=1}^{\frac{p-1}{2}} (-1)^m S_m(r) \\ &= \alpha_0 + \sum_{\substack{0 < n < p \\ \chi(n) = -1}} \alpha_n + \sum_{\substack{0 < r < p \\ \chi(r) = +1}} \alpha_r = \alpha_0 + \frac{p-1}{2}(\alpha_N + \alpha_R) \end{aligned}$$

が成り立つ. 一方 $\sum_{m=1}^{\frac{p-1}{2}} (-1)^m |V_m| = \sum_{m=1}^{\frac{p-1}{2}} (-1)^m \binom{\frac{p-1}{2}}{m} = -1$ なので命題が成り立つ.

命題 4.5. 次が成り立つ:

$$N(\theta) + R(\theta) = \frac{2p}{p-1}(1 + \alpha_0).$$

証明. 命題 4.2 より $R(\theta) = 1 + \alpha_0 + \sum_{\substack{0 < n < p \\ \chi(n) = -1}} \alpha_n \theta^n + \sum_{\substack{0 < r < p \\ \chi(r) = +1}} \alpha_r \theta^r = 1 + \alpha_0 + \alpha_N \sum_{\substack{0 < n < p \\ \chi(n) = -1}} \theta^n$

$+\alpha_R \sum_{\substack{0 < r < p \\ \chi(r)=+1}} \theta^r$ であり, また $\chi(s) = -1$ なる s に対して $N(\theta) = R(\theta^s)$ に注意すると

$$N(\theta) = 1 + \alpha_0 + \alpha_N \sum_{\substack{0 < n < p \\ \chi(n)=-1}} \theta^{sn} + \alpha_R \sum_{\substack{0 < r < p \\ \chi(r)=+1}} \theta^{sr} = 1 + \alpha_0 + \alpha_N \sum_{\substack{0 < r < p \\ \chi(r)=+1}} \theta^r + \alpha_R \sum_{\substack{0 < n < p \\ \chi(n)=-1}} \theta^n$$

成り立つ.

$$\text{ゆえに } \sum_{\substack{0 < n < p \\ \chi(n)=-1}} \theta^n + \sum_{\substack{0 < r < p \\ \chi(r)=+1}} \theta^r = \sum_{k=1}^{p-1} \theta^k = -1 \text{ および命題 4.4 より}$$

$$N(\theta) + R(\theta) = 2(1 + \alpha_0) + \frac{2}{p-1}(1 + \alpha_0) = \frac{2p}{p-1}(1 + \alpha_0)$$

が成り立つ.

命題 4.6. 次が従う:

$$\alpha_0 = -\frac{1}{p} + \frac{p-1}{2p} \sum_{m=1}^{\frac{p-1}{2}} (-1)^m \frac{1}{m!} H(m).$$

証明. 各 $1 \leq m \leq (p-1)/2$ に対して

$$\begin{aligned} \mathcal{DN}_m^\times &= \left\{ \left(t_1, t_2, \dots, t_m \right) \in \mathbf{F}_p^m \left| \begin{array}{l} t_1^2 + t_2^2 + \dots + t_m^2 = 0, \\ t_i \neq 0 \ (1 \leq i \leq m), \\ t_i^2 \neq t_j^2 \ (1 \leq i < j \leq m) \end{array} \right. \right\} \\ &= 2^m \left\{ \left(t_1, t_2, \dots, t_m \right) \left| \begin{array}{l} t_1 + t_2 + \dots + t_m \equiv 0 \pmod{p}, \\ \chi(t_i) = 1 \ (1 \leq i \leq m), \\ t_i \not\equiv t_j \pmod{p} \ (1 \leq i < j \leq m) \end{array} \right. \right\} \\ &= 2^m m! \left\{ \left(t_1, t_2, \dots, t_m \right) \left| \begin{array}{l} t_1 + t_2 + \dots + t_m \equiv 0 \pmod{p}, \\ \chi(t_i) = 1 \ (1 \leq i \leq m), \\ 1 \leq t_1 < t_2 < \dots < t_m \leq p-1 \end{array} \right. \right\} \\ &= 2^m m! S_m(0) \end{aligned}$$

なので, $S_m(0) = (1/2^m)(1/m!) \mathcal{DN}_m^\times$ ($1 \leq m \leq (p-1)/2$) が成り立つ.

ゆえに命題 3.6 より

$$\begin{aligned} \alpha_0 &= \sum_{m=1}^{\frac{p-1}{2}} (-1)^m S_m(0) = \sum_{m=1}^{\frac{p-1}{2}} (-1)^m \frac{1}{2^m} \frac{1}{m!} \mathcal{DN}_m^\times \\ &= \frac{1}{p} \left\{ \sum_{m=1}^{\frac{p-1}{2}} (-1)^m \binom{\frac{p-1}{2}}{m} + \frac{1}{2}(p-1) \sum_{m=1}^{\frac{p-1}{2}} (-1)^m \frac{1}{m!} H(m) \right\} \\ &= -\frac{1}{p} + \frac{p-1}{2p} \sum_{m=1}^{\frac{p-1}{2}} (-1)^m \frac{1}{m!} H(m) \end{aligned}$$

が成り立つ.

次に $q_i = (1 + \chi(i)\sqrt{p})/2$ ($1 \leq i \leq (p-1)/2$) とおき, また実 2 次体 $Q(\sqrt{p})$ の整数 x に対してその共役元を \bar{x} で表す.

命題 4.7. 各 $1 \leq m \leq (p-1)/2$ に対して

$$(-1)^m \frac{1}{m!} H(m) = \mathcal{I}_m(q_1, q_2, \dots, q_m) + \mathcal{I}_m(\bar{q}_1, \bar{q}_2, \dots, \bar{q}_m)$$

を得る.

証明. $v_A = v(|A_1|, |A_2|, \dots, |A_{w_A}|) = |\{A_i; \chi(|A_i|) = -1\}| = \sum_{\substack{1 \leq i \leq n \\ \chi(i) = -1}} c_i^A$ および $w_A - v_A$
 $= |\{A_i; \chi(|A_i|) = +1\}| = \sum_{\substack{1 \leq i \leq n \\ \chi(i) = +1}} c_i^A$ に注意すると,

$$\begin{aligned} D_{w_A}(v_A) &= (1 + \sqrt{p})^{w_A - v_A} (1 - \sqrt{p})^{v_A} + (1 + \sqrt{p})^{v_A} (1 - \sqrt{p})^{w_A - v_A} \\ &= \prod_{\substack{1 \leq i \leq n \\ \chi(i) = +1}} (1 + \sqrt{p})^{c_i^A} \prod_{\substack{1 \leq i \leq n \\ \chi(i) = -1}} (1 - \sqrt{p})^{c_i^A} + \prod_{\substack{1 \leq i \leq n \\ \chi(i) = -1}} (1 + \sqrt{p})^{c_i^A} \prod_{\substack{1 \leq i \leq n \\ \chi(i) = +1}} (1 - \sqrt{p})^{c_i^A} \\ &= \prod_{1 \leq i \leq n} (1 + \chi(i)\sqrt{p})^{c_i^A} + \prod_{1 \leq i \leq n} (1 - \chi(i)\sqrt{p})^{c_i^A} \end{aligned}$$

が成り立つ.

ゆえに補題 2.6, 2.8 および系 2.7.1 より各 $1 \leq m \leq (p-1)/2$ に対して

$$\begin{aligned} (-1)^m \frac{1}{m!} H(m) &= (-1)^m \frac{1}{m!} \sum_{A \in \mathcal{P}_m} (-1)^{w_A} \frac{1}{2^{w_A}} D_{w_A}(v_A) \mu(0, A) \\ &= (-1)^m \frac{1}{m!} \sum_{A \in \mathcal{P}_m} \left[(-1)^{w_A} \frac{1}{2^{\sum_{i=1}^m c_i^A}} \left\{ \prod_{i=1}^m (1 + \chi(i)\sqrt{p})^{c_i^A} \right. \right. \\ &\quad \left. \left. + \prod_{i=1}^m (1 - \chi(i)\sqrt{p})^{c_i^A} \right\} (-1)^{m+w_A} \prod_{i=1}^m \{(i-1)!\}^{c_i^A} \right] \\ &= \frac{1}{m!} \sum_{A \in \mathcal{P}_m} \left\{ \prod_{i=1}^m \{(i-1)!\}^{c_i^A} \right\} \left\{ \prod_{i=1}^m q_i^{c_i^A} + \prod_{i=1}^m \bar{q}_i^{c_i^A} \right\} \\ &= \frac{1}{m!} \sum_m^* \frac{m!}{\prod_{i=1}^m \{c_i! \cdot (i!)^{c_i}\}} \left\{ \prod_{i=1}^m \{(i-1)!\}^{c_i^A} \right\} \left\{ \prod_{i=1}^m q_i^{c_i^A} + \prod_{i=1}^m \bar{q}_i^{c_i^A} \right\} \\ &= \frac{1}{m!} \sum_m^* \frac{m!}{\prod_{i=1}^m \{c_i! \cdot i^{c_i}\}} \left\{ \prod_{i=1}^m q_i^{c_i^A} + \prod_{i=1}^m \bar{q}_i^{c_i^A} \right\} \\ &= \mathcal{I}_m(q_1, q_2, \dots, q_m) + \mathcal{I}_m(\bar{q}_1, \bar{q}_2, \dots, \bar{q}_m) \end{aligned}$$

が成り立つ.

命題 4.8. 次が従う:

$$N(\theta) + R(\theta) = \sum_{m=0}^{\frac{p-1}{2}} \{ \mathcal{I}_m(q_1, q_2, \dots, q_m) + \mathcal{I}_m(\bar{q}_1, \bar{q}_2, \dots, \bar{q}_m) \}.$$

証明. 命題 4.6, 4.7, 3.8 および $\mathcal{I}_0 = 1$ に注意すると,

$$\begin{aligned} N(\theta) + R(\theta) &= \frac{2p}{p-1}(1 + \alpha_0) = 2 + \sum_{m=1}^{\frac{p-1}{2}} (-1)^m \frac{1}{m!} H(m) \\ &= 2 + \sum_{m=1}^{\frac{p-1}{2}} \{ \mathcal{I}_m(q_1, q_2, \dots, q_m) + \mathcal{I}_m(\bar{q}_1, \bar{q}_2, \dots, \bar{q}_m) \} \\ &= \sum_{m=0}^{\frac{p-1}{2}} \{ \mathcal{I}_m(q_1, q_2, \dots, q_m) + \mathcal{I}_m(\bar{q}_1, \bar{q}_2, \dots, \bar{q}_m) \} \end{aligned}$$

が成り立つ.

定理 1 の証明. $\mathcal{I}_n(q_1, q_2, \dots, q_n) = (a_n + b_n\sqrt{p})/2$ ($n \geq 0$) とおくと, $\mathcal{I}_n(\bar{q}_1, \bar{q}_2, \dots, \bar{q}_n) = (a_n - b_n\sqrt{p})/2$ に注意して

$$N(\theta) + R(\theta) = \sum_{m=0}^{\frac{p-1}{2}} \{ \mathcal{I}_m(q_1, q_2, \dots, q_m) + \mathcal{I}_m(\bar{q}_1, \bar{q}_2, \dots, \bar{q}_m) \} = \sum_{m=0}^{\frac{p-1}{2}} a_m$$

なので, 命題 4.1 より

$$T = \frac{\{N(\theta) + R(\theta)\}^2}{p} - 2 = \frac{1}{p} \left\{ \sum_{m=0}^{\frac{p-1}{2}} a_m \right\}^2 - 2$$

が成り立つ.

また a_n, b_n ($n \geq 0$) に関する漸化式については,

$$\begin{aligned} a_n &= \{ \mathcal{I}_n(q_1, q_2, \dots, q_n) + \mathcal{I}_n(\bar{q}_1, \bar{q}_2, \dots, \bar{q}_n) \} \quad (n \geq 0), \\ b_n &= \frac{1}{\sqrt{p}} \{ \mathcal{I}_n(q_1, q_2, \dots, q_n) - \mathcal{I}_n(\bar{q}_1, \bar{q}_2, \dots, \bar{q}_n) \} \quad (n \geq 0) \end{aligned}$$

および補題 2.9 よりわかる.

例. $p = 229$ のとき, 各 a_n, b_n ($n \geq 0$) は表 1 のようになり, これより $T = 11696402$ がわかる. ゆえにペル方程式 $T^2 - pU^2 = 4$ より $\varepsilon^{2h} = \frac{11696402 + 772920\sqrt{229}}{2}$ となり, $\varepsilon = \frac{15 + \sqrt{229}}{2}$ なので $h = 3$ がわかる.

注意. $N = (p-1)/4$ とおくととき, 定理 2 の中の d_n ($1 \leq n \leq N$) は定理 1 の中の a_n, b_n ($1 \leq n \leq N$) を使って

$$d_n = \frac{a_n + b_n\sqrt{p}}{2} \quad (1 \leq n \leq N)$$

と表せ, さらに $\mathcal{I}_n(q_1, q_2, \dots, q_n) = (a_n + b_n\sqrt{p})/2$ より

$$d_n = \mathcal{I}_n(q_1, q_2, \dots, q_n) \quad (1 \leq n \leq N)$$

とも表せる.

References

- [1] P. CHOWLA, *On the class-number of real quadratic fields*, J. Reine Angew. Math. **230** (1968), 51-60.
- [2] G. FUJISAKI, *Field theory and Galois theory*, Iwanami Pub., Tokyo (1977).
- [3] H. HASSE, *Vorlesungen über Zahlentheorie*, Springer Verlag, Berlin Göttingen Heidelberg New York(1964).
- [4] L. LOVÁSZ, *Combinatorial Problems and Exercises*, Akadémiai Kiadó, Budapest (1979), Japanese Ed. translated by H. Narushima, M. Tuchiya, Tokai Univ. Pub. Tokyo (1988).
- [5] T. MITSUHIRO, *A Combinatorial Deformation of Dirichlet's Class Number Formula*, Rep. Fac. Sci. Engrg. Saga Univ. Math. **22**(1993), 1-19.
- [6] T. ONO, *A deformation of Dirichlet's class number formula*, In: Algebraic Analysis, Vol II, (M. Kashiwara and T. Kawai, eds), Academic Press, Boston(1988), 659-666.
- [7] G. PÓLYA, R. E. TARJAN and D. R. WOODS, *Note on Introductory Combinatorics*, Birkhäuser, Boston (1983), Japanese Ed. translated by A. Imamiya, Kindai Kagakusya, Tokyo (1986).
- [8] R. T. STANLEY, *Enumerative Combinatorics, Vol. 1*, Wadsworth & Brooks/Cole Advanced Books, Monterey (1986), Japanese Ed. translated by H. Narushima, H. Yamada, K. Watanabe and A. Shimizu, Nippon Hyoron-sya, Tokyo (1990).

Graduate School of Science and Engineering
 Saga University
 Saga 840, Japan

E-mail address: mituhiro@ms.saga-u.ac.jp

表 1. $p = 229$ のときの各 a_n, b_n の値

n	a_n	b_n	n	a_n	b_n	n	a_n	b_n
0	2	0	39	-165264	10980	78	159903	-10495
1	1	1	40	167890	-11000	79	-156200	10366
2	58	0	41	-167520	11186	80	153640	-10108
3	-28	10	42	170221	-11151	81	-149006	9924
4	319	-9	43	-169978	11308	82	146081	-9553
5	-377	41	44	172284	-11308	83	-139635	9331
6	1162	-52	45	-172428	11470	84	135714	-8854
7	-1440	134	46	174828	-11502	85	-127618	8568
8	3230	-164	47	-175794	11642	86	122939	-7981
9	-4023	317	48	177681	-11725	87	-113552	7644
10	6861	-399	49	-179033	11839	88	108099	-7001
11	-8492	630	50	180508	-11936	89	-98131	6623
12	12739	-761	51	-182022	12020	90	92002	-5968
13	-15275	1081	52	183367	-12105	91	-82390	5528
14	20512	-1302	53	-184320	12204	92	75443	-4905
15	-24613	1681	54	185695	-12257	93	-66050	4448
16	31109	-1987	55	-186359	12329	94	59138	-3846
17	-36317	2463	56	187342	-12340	95	-50669	3383
18	43894	-2862	57	-186804	12402	96	43894	-2862
19	-50669	3383	58	187342	-12340	97	-36317	2463
20	59138	-3846	59	-186359	12329	98	31109	-1987
21	-66050	4448	60	185695	-12257	99	-24613	1681
22	75443	-4905	61	-184320	12204	100	20512	-1302
23	-82390	5528	62	183367	-12105	101	-15275	1081
24	92002	-5968	63	-182022	12020	102	12739	-761
25	-98131	6623	64	180508	-11936	103	-8492	630
26	108099	-7001	65	-179033	11839	104	6861	-399
27	-113552	7644	66	177681	-11725	105	-4023	317
28	122939	-7981	67	-175794	11642	106	3230	-164
29	-127618	8568	68	174828	-11502	107	-1440	134
30	135714	-8854	69	-172428	11470	108	1162	-52
31	-139635	9331	70	172284	-11308	109	-377	41
32	146081	-9553	71	-169978	11308	110	319	-9
33	-149006	9924	72	170221	-11151	111	-28	10
34	153640	-10108	73	-167520	11186	112	58	0
35	-156200	10366	74	167890	-11000	113	1	1
36	159903	-10495	75	-165264	10980	114	2	0
37	-161227	10733	76	164378	-10804			
38	164378	-10804	77	-161227	10733			