

Hecke operators の計算について

上智大 理工 和田秀男

Hecke operators の具体的な働きを計算するには、多項式の因数分解と虚2次体の類数を計算しなければならないので、まずこの2点について述べよう。

§ 1. 因数分解

有理整数を係数とする多項式：

$$F(x) = x^n + k_1 x^{n-1} + k_2 x^{n-2} + \cdots + k_n, \quad k_i \in \mathbb{Z}$$

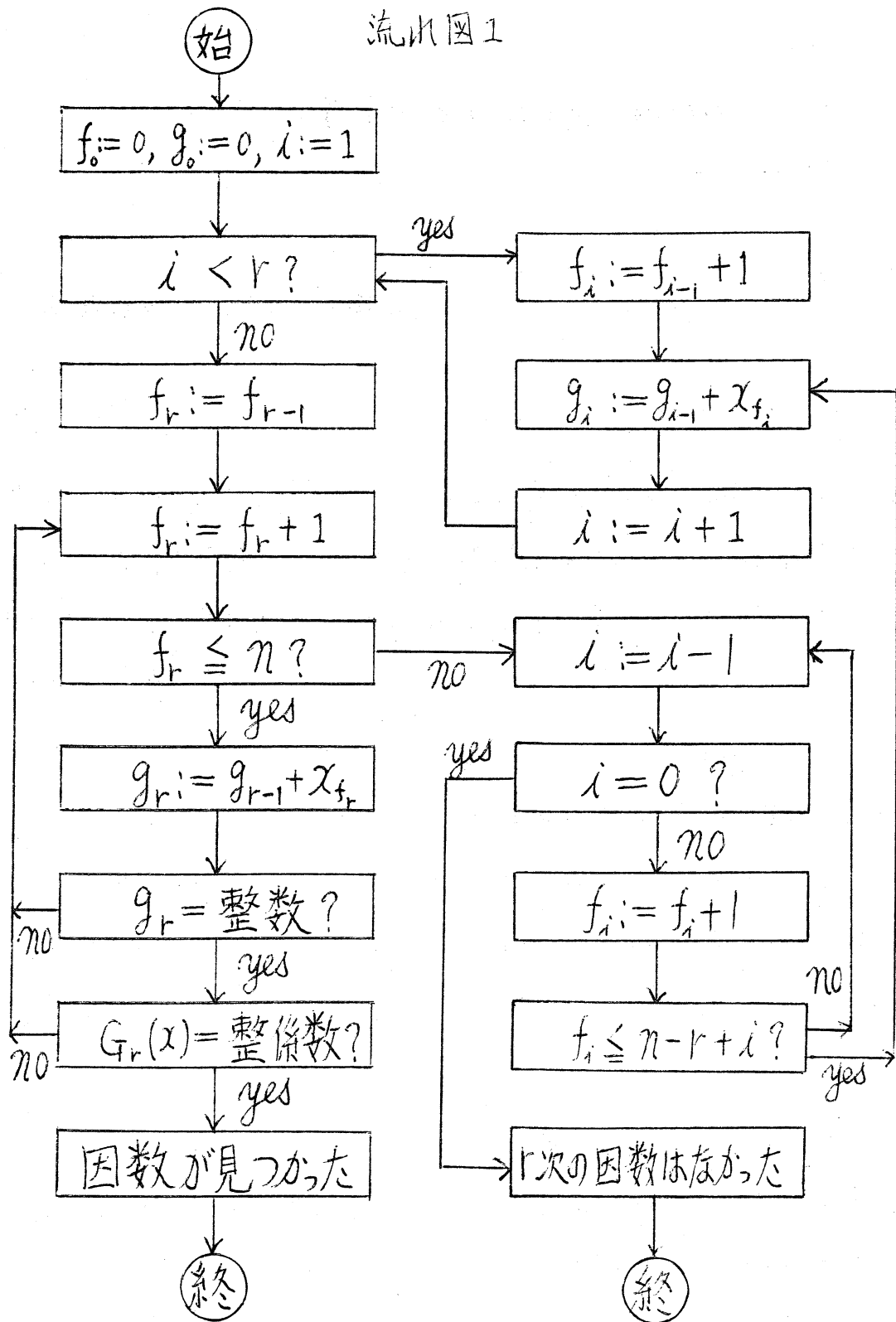
を因数分解するには、 $F(x) = 0$ の根 $x_1, x_2, \dots, x_n$ の中より、 r 個 ($1 \leq r \leq \frac{n}{2}$) $x_{f_1}, x_{f_2}, \dots, x_{f_r}$ を選び出し、

$$G_r(x) = (x - x_{f_1})(x - x_{f_2}) \cdots (x - x_{f_r})$$

が整係数になるかどうかをすべての組み合わせで調べれば良い。そのためにはまず

$$g_r = x_{f_1} + x_{f_2} + \cdots + x_{f_r}$$

流水図 1



を計算し、 g_r が整数のとき $G_r(x)$ を計算すれば良い。1個を選ぶすべての組み合わせを作る方法は流れ図1のようにする。実例として

$$\begin{aligned} F(x) = & x^{10} + 79x^9 + 2850x^8 + 62285x^7 + 922386x^6 \\ & + 9808357x^5 + 77456063x^4 + 463047814x^3 \\ & + 2117748840x^2 + 7436199023x + 20000201335 \\ & + 40864981130x + 62492846639x \\ & + 69863925734x^5 + 55066595198x^4 \\ & + 28885227055x^3 + 9115502993x^2 + 1395936512x \\ & + 47367833 \end{aligned}$$

のとき、まず $F(x) = 0$ の根を計算してみると、すべて負根で近似値は

$$x_1 = -10.989395213965386179360830791621$$

$$x_2 = -10.372176552914877482949302815600$$

$$x_3 = -8.685121751541672674194381989894$$

$$x_4 = -7.790274736615651531405170850597$$

$$x_5 = -6.407976666889782759819381752687$$

$$x_6 = -6.180916186419658304393214101654$$

$$x_7 = -4.803782605994559553743521163324$$

$$x_8 = -4.329714748494450426992750972764$$

$$x_9 = -4.01331497413821386549477588338$$

$$x_{10} = -3.760759918313082884859161416599$$

$$x_{11} = -3.076633415807948648243626338657$$

$$x_{12} = -2.912905747858908671900026127493$$

$$x_{13} = -1.691686182740750911904474618406$$

$$x_{14} = -1.355398050062112877608746936355$$

$$x_{15} = -1.313908957870019177985426579568$$

$$x_{16} = -0.698277464713688278924782188167$$

$$x_{17} = -0.571944785946945410300740033498$$

$$x_{18} = -0.045812039712290359919350911941$$

となった。この値をもとにして r 個 ($1 \leq r \leq 9$) の根の和ですべての組み合わせで調べてみるとどれも整数にならなかった。整数か否かは、小数点以下 8 個 0 がつくか、または 8 個 9 がつくかで判定した。最後に根の近似値を使って用心深く $(x-x_1)(x-x_2) \cdots (x-x_8)$ を計算してみると

$$= x^8 + 78.999999999999999999999999667177186x'^7$$
$$+ 2849.999999999999999999999999752218180x'^6$$
$$+ 62284.999999999999999999999999163974924x'^5$$
$$+ 922385.99999999999999999999998305786192x'^4$$
$$+ 9809356.99999999999999999999997695910104x'^3$$
$$+ 77456062.9999999999999999999999774353944x'^2$$

$$\begin{aligned}
& + 463047813.99999999999998423619534 x'' \\
& + 2117748839.9999999999999166733150 x^{10} \\
& + 7436199022.9999999999996685876174 x^9 \\
& + 20000201334.999999999999007498180 x^8 \\
& + 40864981129.999999999997775447950 x^7 \\
& + 62492846638.999999999996317573466 x^6 \\
& + 69863925733.999999999995597032842 x^5 \\
& + 55066595197.999999999996328720586 x^4 \\
& + 28885227054.999999999997983037900 x^3 \\
& + 9115502992.9999999999993395083560 x^2 \\
& + 1395936511.9999999999998960104250 x \\
& + 47367832.999999999999996443617034
\end{aligned}$$

となった。よって整数か否かの判定を8個0または9がな
ぶか否かで調べたのは安全な方法であったことがわかる。つ
まり $F(x)$ は既約である。根を計算する時間を別にすれば、
津田塾大学にある小型計算機 TOSBAC-3000 で35秒で、
 $F(x)$ が既約だと判定された。

§ 2. 虚2次体の類数

自然数 d_0 を素数の2乗で割れない数とする。このとき

$$d = \begin{cases} d_0, & d_0 \equiv 3 \pmod{4} \text{ のとき} \\ 4d_0, & d_0 \not\equiv 3 \pmod{4} \text{ のとき} \end{cases}$$

と d を定める。 $(-d)$ を判別式に持つ虚 2 次体の類数

$$h = h(-d) \text{ とは}$$

$$(1) \quad b^2 - 4ac = -d$$

$$(2) \quad |b| \leq a \leq c$$

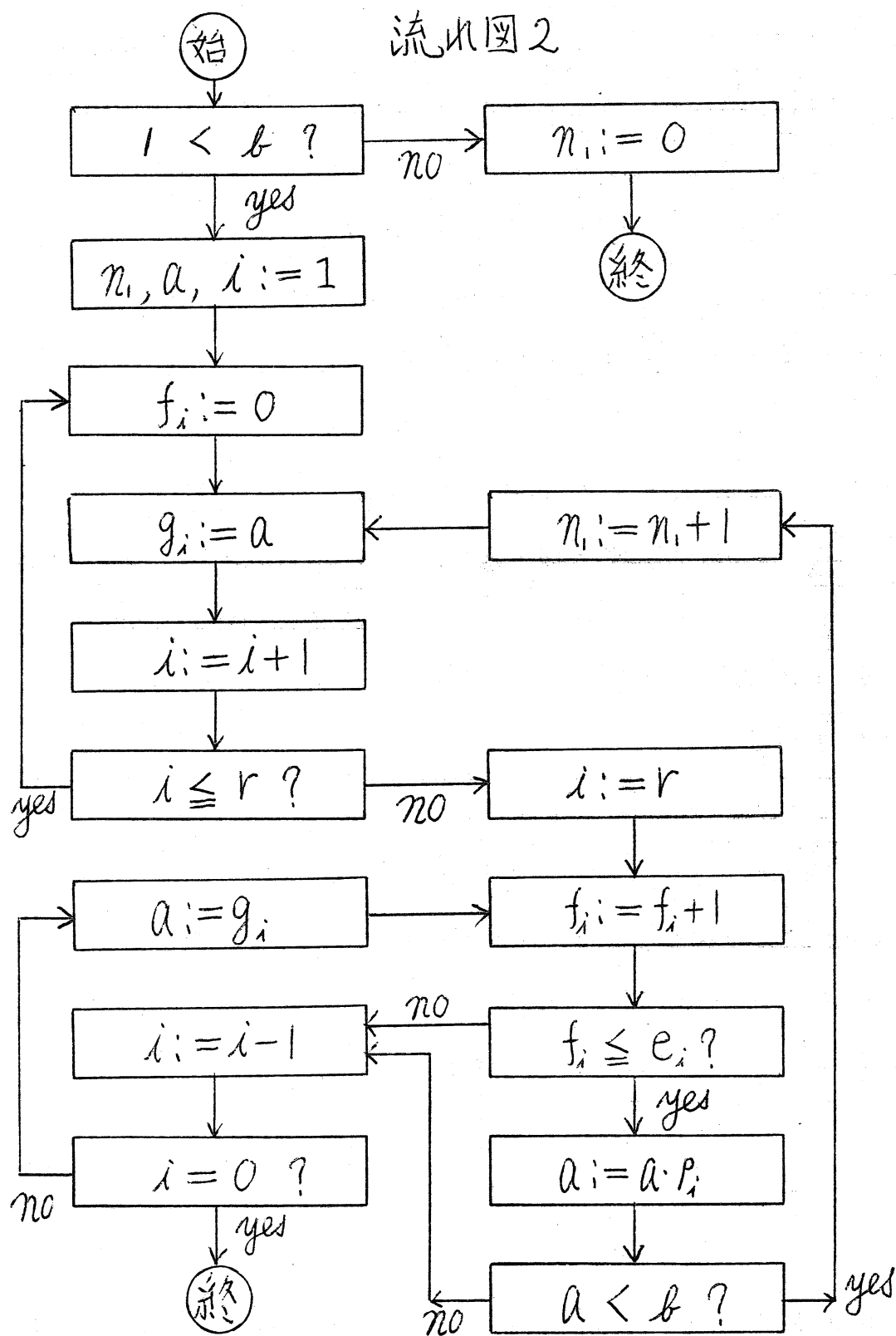
を満たす整数 a, b, c の組み合わせの個数である。ただし $|b| = a$ または $a = c$ が成り立つときは、 b は正の値のみに限る。

さてこのとき $-d = b^2 - 4ac \leq b^2 - 4b \cdot b = -3b^2$,
したがって $b^2 \leq d/3$ となる。 $b (\geq 0)$ を固定したとき、
 $y = (b^2 + d)/4$ とおくと、 a, c は y の約数である。いかに能率的に a, c の組み合わせの個数を求めるか、考えてみよう。

(A) $b = 0$ のとき、 y の約数の個数を n とすると $y = a \cdot c$, $a \leq c$ となる組み合わせの個数は $[(n+1)/2]$ 通りである。

(B) $b \neq 0$ のとき、 y の約数の個数を n , そのうち b より小さくなる個数を n_1 とすれば、
($y = a \cdot c$, $b < a < c$ となる a, c の組み合わせ) $\times 2$ + ($y = a \cdot c$, $b = a$ または $a = c$ となる a, c の組み合わせ) は

流程图 2



$l \nmid y$ または $l^2 = y = 1$ のとき $(n - 2n_1)$ 通り,

$l \mid y$, $l^2 < y$ のとき $(n - 2n_1 - 1)$ 通りとなる。

以上より、類数 $h(-d)$ を計算するには、 y を

$$y = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \quad p_i = \text{素数}$$

と素因子分解し、その約数の個数 $n = \prod_{i=1}^r (1 + e_i)$ を計算するプログラムが与えなければならない。次に y の約数

$$a = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}, \quad (0 \leq f_i \leq e_i)$$

の中に $a < l$ となる a の個数 n_l を計算するプログラムが必要である。 n_l は流れ図で計算される。この図において g_i は

$$g_i = p_1^{f_1} p_2^{f_2} \cdots p_i^{f_i}$$

のつもりである。

§ 3. Hecke operators の計算

Hecke operator $T(m)$ とはあるベクトル空間 $V(q)$ より $V(q)$ への線型写像である。しかも $V(q)$ の base を適当に (m に無関係に) 選ぶと

$$T(m) = \begin{pmatrix} x_1 & & 0 \\ & x_2 & \\ & & \ddots \\ 0 & & & x_n \end{pmatrix}$$

と表わされること、知られている。 $x_1, x_2, \dots, x_n$ を

求めることが目的だけだと、Eichler の公式により

$$\text{tr } T(m) = x_1 + x_2 + \cdots + x_n = \sum_{d^2-4m < 0} A(d, m) \cdot h(d^2-4m) + B(m)$$

と表わされることが知られている。\$A(d, m)\$, \$B(m)\$ は容易に計算出来る \$d, m\$ の関数である。よって類数 \$h(d^2-4m)\$ が求まれば \$\text{tr } T(m) = x_1 + x_2 + \cdots + x_n\$ は計算出来る。次に志村公式

$$T(P)^k = \sum_{0 \leq r \leq \frac{k}{2}} \left\{ \binom{k}{r} - \binom{k}{r-1} \right\} \cdot P^r \cdot T(P^{k-2r}), \quad (P = \text{素数}, \binom{n}{-1} = 0)$$

を用いれば \$\text{tr } T(P)\$, \$\dots\$, \$\text{tr } T(P^n)\$ より \$\text{tr } T(P)^2\$, \$\dots\$, \$\text{tr } T(P)^n\$ が計算出来る。つまり

$$T(P) = \begin{pmatrix} x_1 & & 0 \\ x_2 & & \\ & \ddots & \\ 0 & & x_n \end{pmatrix}$$

としたとき、\$x_1 + x_2 + \cdots + x_n\$, \$x_1^2 + x_2^2 + \cdots + x_n^2\$, \$\dots\$, \$x_1^n + x_2^n + \cdots + x_n^n\$ が求まる。これらより Newton 公式を用いれば、\$x_1, x_2, \dots, x_n\$ を根とする方程式が定まる。よって \$x_1, x_2, \dots, x_n\$ の近似値が計算出来る。またその方程式を因数分解することにより、\$T(P)\$ の作用の仕方がより明かになる。一般の \$m\$ に対しては

$$(1) \quad T(m_1 \cdot m_2) = T(m_1) \cdot T(m_2), \quad (m_1, m_2) = 1$$

$$(2) \quad T(P^k) = T(P) \cdot T(P^{k-1}) - P \cdot T(P^{k-2}), \quad P = \text{素数}$$

を用いなければならない。

ところで d が大きいと、 $h(-d)$ を計算するのに時間がかかる。また、 m が大きいと $d^2 - 4m < 0$ となる λ の個数も多くなる。例えば $q = 239$ のとき $\dim V(q) = 20$ 、よって $T(2)$ を求めるには、 $\text{tr} T(2)$, $\text{tr} T(2^2)$, $\dots$, $\text{tr} T(2^{20})$ を計算しなければならない。 $\text{tr} T(2^{20})$ を計算するには、TOSBAC-3000 で約 1 時間かかる。 $\text{tr} T(m)$ を求める時間は m にほぼ比例するから、正直に $T(3)$ を求めるために $\text{tr} T(3^{20})$ を計算すると 400 時間位かかってしまう。よって次のような工夫をする。まず

$$T(2^k) = \begin{pmatrix} a_1^{(k)} & & 0 \\ a_2^{(k)} & & \\ & \ddots & \\ 0 & & a_{20}^{(k)} \end{pmatrix}, \quad T(3) = \begin{pmatrix} y_1 & & 0 \\ y_2 & & \\ & \ddots & \\ 0 & & y_{20} \end{pmatrix}$$

とおく。 $T(2)$ がわかれば $T(2^k)$ は $T(2)$ より計算出来る。次に (1) を用いれば

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1^{(1)} & a_2^{(1)} & \dots & a_{20}^{(1)} \\ \vdots & & & \\ a_1^{(19)} & a_2^{(19)} & \dots & a_{20}^{(19)} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{20} \end{pmatrix} = \begin{pmatrix} \text{tr} T(3) \\ \text{tr} T(2 \cdot 3) \\ \vdots \\ \text{tr} T(2^{19} \cdot 3) \end{pmatrix}$$

となるので、この連立方程式を解けば $T(3)$ が求まる。同様に $T(5)$ を求めるには $\text{tr} T(5)$, $\text{tr} T(2 \cdot 5)$, $\dots$,

$tuT(2^{10} \cdot 5)$, $tuT(3 \cdot 5)$, $\dots$, $tuT(3^9 \cdot 5)$ を計算すれば
 良い。このように $T(1)$, $T(2)$, $T(3)$, $\dots$, $T(20)$ が求ま
 れば、 $T(P)$, ($P > 20$) は $tuT(P)$, $tuT(2P)$, $tuT(3P)$,
 $\dots$, $tuT(20P)$ を計算すれば求まる。結局 $T(2)$, $T(3)$
 を求めるのに時間がかかり、他は桁違いに早く計算出来るわ
 けである。