1 Number theoretic transform の導出

n, m を自然数とし，$N = 2^m$ とする．$R = \mathbb{Z}/n\mathbb{Z}$ は $\omega_N^N = 1$ を満たす $\omega_N \in R$ をもつとする．$(f_k)_{k=0,1,\ldots,N-1}$ を R の点列とし，

$$F_k = \sum_{j=0}^{N-1} \omega_N^{jk} f_j, \quad k = 0, 1, \ldots, N-1 \tag{1.1}$$

とする．本稿では，(f_k) から (F_k) の効率的な計算方法について述べる．素朴に計算をすれば，ω_N^{jk} の計算が $O(1)$ であってさえ，全体の計算量は $O(N^2)$ である．

Lemma 1.1. n, m を自然数とし，$N = 2^m$ とする．$R = \mathbb{Z}/n\mathbb{Z}$ は $\omega_N^N = 1$ を満たす $\omega_N \in R$ をもつとする．このとき，$0 \leqslant l \leqslant m$ について，$\omega_{N/2^l}^{N/2^l} = 1$ を満たす $\omega_{N/2^l} \in R$ が存在する．

Proof. $0 \leqslant l \leqslant m$ とする．$(\omega_N^{2^{m-l}})^{2^l} = \omega_N^{2^m} = \omega_N^N = 1$ より，$\omega_{N/2^l} = \omega_N^{2^{m-l}} \in R$ である． □

Lemma 1.2. $l = 0, 1, \ldots, m-1$ について，$\omega_{N/2^l}^2 = \omega_{N/2^{l+1}}$ である．

Proof. $l = 0, 1, \ldots, m-1$ とする．$(\omega_{N/2^l}^2)^{N/2^{l+1}} = \omega_{N/2^l}^{N/2^l} = 1$ である． □

Lemma 1.3. $l = 0, 1, \ldots, m-1$ について，$\omega_{N/2^l}^{N/2^{l+1}} = -1$ である．

Proof. $l = 0, 1, \ldots, m-1$ とする．$(\omega_{N/2^l}^{N/2^{l+1}})^2 = \omega_{N/2^l}^{N/2^l} = 1$ である．よって，$\omega_{N/2^l}^{N/2^{l+1}} = -1$ である． □

Proposition 1.1. $0 \leqslant k \leqslant N/2 - 1$ とする．F_k^e, F_k^o を，

$$F_k^e = \sum_{j=0}^{N/2-1} \omega_{N/2}^{jk} f_{2j}, \tag{1.2}$$

$$F_k^o = \sum_{j=0}^{N/2-1} \omega_{N/2}^{jk} f_{2j+1} \tag{1.3}$$

とすると，

$$F_k = F_k^e + \omega^k F_k^o, \tag{1.4}$$

$$F_{k+N/2} = F_k^e - \omega^k F_k^o, \tag{1.5}$$

が成り立つ．

Proof.

$$\begin{aligned}
F_k &= \sum_{j=0}^{N-1} \omega_N^{jk} f_j \\
&= \sum_{j=0,2,\ldots,N-2} \omega_N^{jk} f_j + \sum_{j=1,3,\ldots,N-1} \omega_N^{jk} f_j \\
&= \sum_{j=0}^{N/2-1} \omega_N^{2jk} f_{2j} + \sum_{j=0}^{N/2-1} \omega_N^{(2j+1)k} f_{2j+1} \\
&= \sum_{j=0}^{N/2-1} (\omega_N^2)^{jk} f_{2j} + \sum_{j=0}^{N/2-1} \omega_N^k (\omega_N^2)^{jk} f_{2j+1}
\end{aligned}$$

であるが，補題 1.2 より，

$$\begin{aligned}
F_k &= \sum_{j=0}^{N-1} \omega_N^{jk} f_j \\
&= \sum_{j=0}^{N/2-1} \omega_{N/2}^{jk} f_{2j} + \omega_N^k \sum_{j=0}^{N/2-1} \omega_{N/2}^{jk} f_{2j+1} \\
&= F_k^e + \omega^k F_k^o
\end{aligned}$$

である．また，

$$\begin{aligned}
&F_{k+N/2} \\
&= \sum_{j=0}^{N-1} \omega_N^{j(k+N/2)} f_j \\
&= \sum_{j=0}^{N/2-1} \omega_{N/2}^{j(k+N/2)} f_{2j} + \omega_N^{k+N/2} \sum_{j=0}^{N/2-1} \omega_{N/2}^{j(k+N/2)} f_{2j+1}
\end{aligned}$$

において，$j = 0, 1, \ldots, N/2-1$ について $\omega_{N/2}^{j(k+N/2)} = \omega_{N/2}^{jk} (\omega_{N/2}^{N/2})^k = \omega_{N/2}^{jk}$ であることと，$\omega_N^{k+N/2} = \omega_N^k \omega_N^{N/2}$ と補題 1.3 より，

$$\begin{aligned}
&F_{k+N/2} \\
&= \sum_{j=0}^{N/2-1} \omega_{N/2}^{jk} f_{2j} - \omega_N^k \sum_{j=0}^{N/2-1} \omega_{N/2}^{jk} f_{2j+1} \\
&= F_k^e - \omega^k F_k^o
\end{aligned}$$

である． □

Theorem 1.1. $1 \leqslant l \leqslant m$ とし，$b_i \in \{e, o\}$, $i = 0, 1, \ldots, l-1$ とする．$B : \{e, o\} \to \{0, 1\}$ を,

$$B(b) = \begin{cases} 0, & b = e, \\ 1, & b = o \end{cases} \tag{1.6}$$

で定める．$F_k^{b_0 b_1 \cdots b_{l-1}}$ を

$$F_k^{b_0 b_1 \cdots b_{l-1}} = \sum_{j=0}^{N/2^l - 1} f_{2^l j + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^l}^{jk} \tag{1.7}$$

とするとき，$0 \leqslant k < N - N/2^{l+1}$, $1 \leqslant l < m$ ならば,

$$\begin{aligned} &F_k^{b_0 b_1 \cdots b_{l-1}} \\ &\quad = F_k^{b_0 b_1 \cdots b_{l-1} e} + \omega_{N/2^l}^k F_k^{b_0 b_1 \cdots b_{l-1} o}, \end{aligned} \tag{1.8}$$

$$\begin{aligned} &F_{k+N/2^{l+1}}^{b_0 b_1 \cdots b_{l-1}} \\ &\quad = F_k^{b_0 b_1 \cdots b_{l-1} e} - \omega_{N/2^l}^k F_k^{b_0 b_1 \cdots b_{l-1} o} \end{aligned} \tag{1.9}$$

が成り立つ．

Proof. $0 \leqslant l < m$ とする．まず,

$$\begin{aligned} &F_k^{b_0 b_1 \cdots b_{l-1}} \\ &= \sum_{j=0}^{N/2^l - 1} f_{2^l j + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^l}^{jk} \\ &= \sum_{j=0,2,\ldots,N/2^l-2} f_{2^l j + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^l}^{jk} \\ &\quad + \sum_{j=1,3,\ldots,N/2^l-1} f_{2^l j + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^l}^{jk} \\ &= \sum_{j=0}^{N/2^{l+1}-1} f_{2^l \cdot 2j + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^l}^{2jk} \\ &\quad + \sum_{j=0}^{N/2^{l+1}-1} f_{2^l (2j+1) + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^l}^{(2j+1)k} \\ &= \sum_{j=0}^{N/2^{l+1}-1} f_{2^{l+1} j + 2^l B(e) + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^{l+1}}^{jk} \\ &\quad + \omega_{N/2^l}^k \sum_{j=0}^{N/2^{l+1}-1} f_{2^{l+1} j + 2^l B(o) + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^{l+1}}^{jk} \\ &= F_k^{b_0 b_1 \cdots b_{l-1} e} + \omega_{N/2^l}^k F_k^{b_0 b_1 \cdots b_{l-1} o} \end{aligned}$$

である．一方,

$$\begin{aligned} &F_{k+N/2^{l+1}}^{b_0 b_1 \cdots b_{l-1}} \\ &= \sum_{j=0}^{N/2^{l+1}-1} f_{2^{l+1} j + 2^l B(e) + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^{l+1}}^{j(k+N/2^{l+1})} \\ &\quad + \omega_{N/2^l}^{k+N/2^{l+1}} \\ &\qquad \times \sum_{j=0}^{N/2^{l+1}-1} f_{2^{l+1} j + 2^l B(o) + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^{l+1}}^{j(k+N/2^{l+1})} \end{aligned}$$

であるが，$\omega_{N/2^{l+1}}^{k+N/2^{l+1}} = \omega_{N/2^{l+1}}^k \omega_{N/2^{l+1}}^{N/2^{l+1}} = \omega_{N/2^{l+1}}^k$ であることと，$\omega_{N/2^l}^{k+N/2^{l+1}} = \omega_{N/2^l}^k \omega_{N/2^l}^{N/2^{l+1}}$ と補題 1.3 より,

$$\begin{aligned} &F_{k+N/2^{l+1}}^{b_0 b_1 \cdots b_{l-1}} \\ &= \sum_{j=0}^{N/2^{l+1}-1} f_{2^{l+1} j + 2^l B(e) + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^{l+1}}^{jk} \\ &\quad - \omega_{N/2^l}^k \\ &\qquad \times \sum_{j=0}^{N/2^{l+1}-1} f_{2^{l+1} j + 2^l B(o) + \sum_{i=0}^{l-1} 2^i B(b_i)} \omega_{N/2^{l+1}}^{jk} \\ &= F_k^{b_0 b_1 \cdots b_{l-1} e} - \omega_{N/2^l}^k F_k^{b_0 b_1 \cdots b_{l-1} o} \end{aligned}$$

である． □

Lemma 1.4. $0 \leqslant k \leqslant N-1$ について，$F_k^{b_0 b_1 \cdots b_{m-1}} = f_{\sum_{j=0}^{m-1} 2^j B(b_j)}$ である．

Proof. 定義より,

$$\begin{aligned} F_k^{b_0 b_1 \cdots b_{m-1}} &= \sum_{j=0}^{0} f_{\sum_{i=0}^{m-1} 2^i B(b_i)} \omega_{N/2^m}^{jk} \\ &= f_{\sum_{j=0}^{m-1} 2^j B(b_j)} \end{aligned}$$

である． □

Theorem 1.2. $\mathcal{B} = B^{-1}$ とする．$R_m : \mathbb{N} \to \mathbb{N}$ を，$k = \sum_{j=0}^{m-1} 2^j a_j$, $a_j \in \{0, 1\}$, $0 \leqslant j \leqslant m-1$ に対して，$R_m(k) = \sum_{j=0}^{m-1} 2^{m-1-j} a_j$ と定める写像とする．

$$F_k^{(0)} = f_{R_m(k)}, \quad k = 0, 1, \ldots, 2^m - 1, \tag{1.10}$$

$$F_k^{(m)} = F_k, \quad k = 0, 1, \ldots, 2^m - 1 \tag{1.11}$$

とする．$0 \leqslant k \leqslant 2^m - 1$, $1 \leqslant l \leqslant m-1$ について，$k = 2^l q + r$, $0 \leqslant r < 2^l$,

$$q = \sum_{j=0}^{m-l-1} 2^j a'_j, \quad a'_j \in \{0, 1\}, \quad 0 \leqslant j \leqslant m-l-1 \tag{1.12}$$

として，

$$F_k^{(l)} = F_r^{\mathcal{B}(a'_{m-l-1})\mathcal{B}(a'_{m-l-2})\cdots\mathcal{B}(a'_0)} \tag{1.13}$$

とする．このとき，$l = 1, 2, \ldots, m$ について，$k = 2^l q + r$, $r = 0, 1, \ldots, 2^{l-1} - 1$, $q = 0, 1, \ldots, 2^{m-l} - 1$ において，

$$F_k^{(l)} = F_k^{(l-1)} + \omega_{N/2^{m-l}}^r F_{k+2^{l-1}}^{(l-1)}, \tag{1.14}$$

$$F_{k+2^{l-1}}^{(l)} = F_k^{(l-1)} - \omega_{N/2^{m-l}}^r F_{k+2^{l-1}}^{(l-1)} \tag{1.15}$$

が成り立つ．

Proof. $l = 1$ のときを示す．$k = 2q, 0 \leqslant q \leqslant 2^{m-2}$ とする．$k = \sum_{j=0}^{m-1} 2^j a_j$ とすると，$a_0 = 0$ であるため，$k = \sum_{j=1}^{m-1} 2^j a_j + 0, k + 1 = \sum_{j=1}^{m-1} 2^j a_j + 1$ であり，$R_m(k+1) = R_m(k) + 2^{m-1} = R_m(k) + N/2$ である．よって，$F_k^{(0)} = f_{R_m(k)}$ および，

$$\begin{aligned}
\omega_{N/2^{m-1}}^k F_{k+1}^{(0)} &= f_{R_m(k)} + \omega_{N/2^{m-1}}^k f_{R_m(k+1)} \\
&= \omega_{N/2^{m-1}}^k f_{R_m(k)+N/2} \\
&= \omega_2^{2q} f_{R_m(k)+N/2} \\
&= (\omega_2^2)^q f_{R_m(k)+N/2} \\
&= f_{R_m(k)+N/2}
\end{aligned}$$

である．一方, $k = 2q, q = \sum_{j=0}^{m-2} 2^j a'_j$ とすると, $a'_j = a_{j+1}$ なので，$\sum_{i=0}^{m-2} 2^{m-2-i} a'_i = \sum_{i=0}^{m-2} 2^{m-2-i} a_{i+1} = \sum_{i=1}^{m-1} 2^{m-1-i} a_i = R_m(k)$ より，

$$\begin{aligned}
F_k^{(1)} &= F_0^{\mathcal{B}(a'_{m-2})\mathcal{B}(a'_{m-3})\cdots\mathcal{B}(a'_0)} \\
&= f_{\sum_{i=0}^{m-2} 2^{m-2-i} a'_i} + \omega_{N/2^{m-1}}^0 f_{2^{m-1} + \sum_{i=0}^{m-2} 2^{m--2-i} a'_i} \\
&= f_{\sum_{i=0}^{m-2} 2^{m-2-i} a'_i} + f_{2^{m-1} + \sum_{i=0}^{m-2} 2^{m-2-i} a'_i} \\
&= f_{R_m(k)} + f_{N/2+R_m(k)} \\
&= F_k^{(0)} + \omega_{N/2^{m-1}}^k F_{k+1}^{(0)}
\end{aligned}$$

によって成り立つ．また，

$$\begin{aligned}
F_{k+1}^{(l)} &= F_1^{\mathcal{B}(a'_{m-2})\mathcal{B}(a'_{m-3})\cdots\mathcal{B}(a'_0)} \\
&= f_{\sum_{i=0}^{m-2} 2^{m-2-i} a'_i} + \omega_{N/2^{m-1}}^1 f_{2^{m-1} + \sum_{i=0}^{m-2} 2^{m-2-i} a'_i} \\
&= f_{\sum_{i=0}^{m-2} 2^{m-2-i} a'_i} + \omega_2^1 f_{2^{m-1} + \sum_{i=0}^{m-2} 2^{m-2-i} a'_i} \\
&= f_{R_m(k)} - f_{N/2+R_m(k)} \\
&= F_k^{(0)} - \omega_{N/2^{m-1}}^k F_{k+1}^{(0)}
\end{aligned}$$

である．

次に，$2 \leqslant l \leqslant m - 1$ とする．$k = 2^l q + r$, $q = \sum_{j=0}^{m-l-1} 2^j a'_j$ とおく．このとき，

$$\begin{aligned}
F_k^{(l)} &= F_r^{\mathcal{B}(a'_{m-l-1})\mathcal{B}(a'_{m-l-2})\cdots\mathcal{B}(a'_0)} \\
&= F_r^{\mathcal{B}(a'_{m-l-1})\mathcal{B}(a'_{m-l-2})\cdots\mathcal{B}(a'_0)e} \\
&\quad + \omega_{N/2^l}^k \\
&\qquad \times F_r^{\mathcal{B}(a'_{m-l-1})\mathcal{B}(a'_{m-l-2})\cdots\mathcal{B}(a'_0)o}
\end{aligned}$$

である．また，$k = 2^{l-1}\hat{q} + \hat{r}, \hat{q} = \sum_{j=0}^{m-l} 2^j \hat{a}'_j$ とおくと，$\hat{a}'_j = 0, \hat{a}'_j = a'_{j-1}, \hat{r} = r$ より，

$$\begin{aligned}
F_k^{(l-1)} &= F_r^{\mathcal{B}(\hat{a}'_{m-l})\mathcal{B}(\hat{a}'_{m-l-1})\cdots\mathcal{B}(\hat{a}'_0)} \\
&= F_r^{\mathcal{B}(\hat{a}'_{m-l})\mathcal{B}(\hat{a}'_{m-l-1})\cdots\mathcal{B}(\hat{a}'_1)e} \\
&= F_r^{\mathcal{B}(a'_{m-l-1})\mathcal{B}(a'_{m-l-2})\cdots\mathcal{B}(a'_0)e}
\end{aligned}$$

かつ，$k + 2^{l-1} = 2^{l-1}(\hat{q} + 1) + \hat{r}$ より，

$$\begin{aligned}
F_{k+2^{l-1}}^{(l-1)} &= F_r^{\mathcal{B}(\hat{a}'_{m-l})\mathcal{B}(\hat{a}'_{m-l-1})\cdots\mathcal{B}(\hat{a}'_1)o} \\
&= F_r^{\mathcal{B}(a'_{m-l-1})\mathcal{B}(a'_{m-l-2})\cdots\mathcal{B}(a'_0)o}
\end{aligned}$$

であるため，

$$F_k^{(l)} = F_k^{(l-1)} + \omega_{N/2^{m-l}}^k F_{k+2^{l-1}}^{(l-1)}$$

が成り立つ．

一方，

$$\begin{aligned}
F_{k+2^{l-1}}^{(l)} &= F_{r+2^{l-1}}^{\mathcal{B}(a'_{m-l-1})\mathcal{B}(a'_{m-l-2})\cdots\mathcal{B}(a'_0)} \\
&= F_{r+N/2^{m-l+1}}^{\mathcal{B}(a'_{m-l-1})\mathcal{B}(a'_{m-l-2})\cdots\mathcal{B}(a'_0)} \\
&= F_r^{\mathcal{B}(a'_{m-l-1})\mathcal{B}(a'_{m-l-2})\cdots\mathcal{B}(a'_0)e} \\
&\quad - \omega_{N/2^{m-l}}^k \\
&\qquad \times F_r^{\mathcal{B}(a'_{m-l-1})\mathcal{B}(a'_{m-l-2})\cdots\mathcal{B}(a'_0)o} \\
&= F_k^{(l-1)} - \omega_{N/2^{m-l}}^k F_{k+2^{l-1}}^{(l-1)}
\end{aligned}$$

である．

最後に，$l = m$ とする．$k = 0, 1, \ldots, 2^{m-1} - 1$ とする．$k = 2^{m-1}0 + k$ より，

$$\begin{aligned}
&F_k^{(m-1)} + \omega_N^k F_{k+2^{m-1}}^{(m-1)} \\
&= F_k^{\mathcal{B}(0)} + \omega_N^k F_k^{\mathcal{B}(1)} \\
&= F_k^e + \omega_N^k F_k^o \\
&= F_k
\end{aligned}$$

$$= F_k^{(m)}$$

であり，

$$\begin{aligned}
&F_{k+2^{m-1}}^{(m)} \\
&= F_{k+2^{m-1}} \\
&= F_k^{\mathcal{B}(0)} - \omega_N^k F_k^{\mathcal{B}(1)} \\
&= F_k^e - \omega_N^k F_k^o \\
&= F_k^{(m-1)} - \omega_N^k F_{k+2^{m-1}}^{(m-1)}
\end{aligned}$$

である．

以上より，すべての $l = 1, 2, \ldots, m$ について，主張が示された． □

Theorem 1.3. 以下の手順で，(f_k) から (F_k) が求まる．ただし，$a \leftarrow b$ で，a の値を b で上書きすることを表す．

1. $(f_0, f_1, \ldots, f_{N-1})$
   $\leftarrow (f_{R_m(0)}, f_{R_m(1)}, \ldots, f_{R_m(N-1)})$
2. (f_k, f_{k+2^l})
   $\leftarrow (f_k + \omega_{N/2^{m-l}}^r f_{k+2^{l-1}}, f_k - \omega_{N/2^{m-l}}^r f_{k+2^{l-1}})$,
   $k = 2^l q + r, \quad r = 0, 1, \ldots, 2^{l-1} - 1$,
   $q = 0, 1, \ldots, 2^{m-l} - 1, \quad l = 1, 2, \ldots, m$
3. $(F_0, F_1, \ldots, F_{N-1}) \leftarrow (f_0, f_1, \ldots, f_{N-1})$.

Proof. これまでのの議論から明らか． □

Proposition 1.2. 定理 1.3 の演算量は，項番 1 の演算量が $O(N \log_2 N)$ であり，$\omega_{N/2^{m-l}}^k$ の演算量が $O(\log_2 N)$ であれば，$O(N \log_2 N)$ である．

Proof. 項番 2 の反復回数が $O(N \log_2 N)$ なので明らか． □

Proposition 1.3. 項番 1 の演算量は $O(N \log_2 N)$ である．

Proof. $r_i = R_m(i), i = 0, 1, \ldots, 2^m - 1$ を求める方法を考える．$0 \leqslant i \leqslant N - 1 = 2^m - 1$ とする．r_{i-1} の最上位ビットが 0 ならば，$i - 1$ は偶数なので，r_i は r_{i-1} の最上位ビットを 1 に変更した値である．つまり，$r_i < 2^{m-1}$ ならば，$r_i = r_{i-1} + 2^{m-1}$ である．次に，r_{i-1} の最上位ビットが 1 ならば，$i - 1$ は奇数なので，r_i 最上位ビットは 0 になり，その次のビットが 0 ならば，それを 1 にすればよい．この場合は，$r_{i-1} \geqslant 2^{m-1}, r_{i-1} < 2^{m-2}, r_i = r_{i-1} - 2^{m-1} + 2^{m-2}$ である．

この要領で，$r_{i-1} \geqslant 2^{m-1}, r_{i-1} \geqslant 2^{m-2}, \ldots, r_{i-1} \geqslant 2^{m-l}, r_{i-1} < 2^{m-l-1}$ ならば，$r_i = r_{i-1} - \sum_{j=1}^{l} 2^{m-j} + 2^{m-l-1}$ である．よって，各 r_i の演算量は $O(\log_2 N)$ なので，全体では $O(N \log_2 N)$ である． □

2 Montgomery 乗算の導出

$N > 0$ を自然数とする．$a, b \in \mathbb{Z}/N\mathbb{Z}$ の積 ab の効率的な計算を考える．$x, y \in \mathbb{Z}$ について，$x \,\%\, y = x - \lfloor x/y \rfloor y$ と定める．

Lemma 2.1. $0 < N < R$, $\gcd(N, R) = 1$ とする．$0 \leqslant T < NR$ とする．$NN' \equiv -1 \pmod R$, $0 \leqslant N' < R$ とする．$t = (T + (TN' \,\%\, R)N)/R$ とする．$t < N$ ならば $t = TR^{-1} \,\%\, N$ であり，$t \geqslant N$ ならば $t - N = TR^{-1} \,\%\, N$ である．

Proof. まず，

$$\begin{aligned}
T + (TN' \,\%\, R)N &= T + \left(TN' - \left\lfloor \frac{TN'}{R} \right\rfloor R\right) N \\
&= T + TNN' - \left\lfloor \frac{TN'}{R} \right\rfloor RN \\
&\equiv T + T \cdot (-1) \pmod R \\
&\equiv 0 \pmod R
\end{aligned}$$

であるため，$(T + (TN' \,\%\, R)N)/R \in \mathbb{Z}$ である．次に，$tR = T + (TN' \,\%\, R)N \equiv T \pmod N$ より，$RR' \equiv 1 \bmod N, 0 \leqslant R' < N$ をみたす R' を R^{-1} と表すと，$t \equiv TR^{-1} \pmod N$ である．

ここで，$T < RN$ であり，$TN' \,\%\, R < R$ より $(TN' \,\%\, R)N < NR$ である．よって，$T + (TN' \,\%\, R)N < 2NR$ より，$t = (T + (TN' \,\%\, R)N)/R < 2N$ である．したがって，$t < N$ ならば $t = TR^{-1} \,\%\, N$ であり，$t \geqslant N$ ならば $t - N = TR^{-1} \,\%\, N$ である． □

Definition 2.1. $0 \leqslant T < NR$ である整数 T について，

$$\mathrm{MR}(T) = \begin{cases} (T + (TN' \,\%\, R)N)/R, & (T + (TN' \,\%\, R)N)/R < N, \\ (T + (TN' \,\%\, R)N)/R - N, & (T + (TN' \,\%\, R)N)/R \geqslant N \end{cases}$$

と定める．

Lemma 2.2. $\mathrm{MR}(T) \equiv TR^{-1} \pmod N$ で，$0 \leqslant \mathrm{MR}(T) < N$ である．

Proof. 明らか． □

Theorem 2.1. $R_2 = R^2 \% N$ とおく．$0 \leqslant a < N$, $0 \leqslant b < N$ について，$A = \mathrm{MR}(aR_2)$, $B = \mathrm{MR}(bR_2)$, $C = \mathrm{MR}(AB)$ とおくと，$\mathrm{MR}(C) = ab \% N$ である．

Proof. $0 \leqslant a < N, 0 \leqslant R_2 < N$ なので，$0 \leqslant aR_2 < N^2 < NR$ であり，同様に $bR_2 < NR$ である．また，$0 \leqslant A < N, 0 \leqslant B < N$ なので，$0 \leqslant AB < N^2 < NR$ である．$R_2R^{-1} \equiv R^2R^{-1} \equiv R \pmod N$ なので，

$$
\begin{aligned}
\mathrm{MR}(C) &\equiv CR^{-1} \pmod N \\
&\equiv \mathrm{MR}(AB)R^{-1} \pmod N \\
&\equiv (ABR^{-1})R^{-1} \pmod N \\
&\equiv \mathrm{MR}(aR_2)\,\mathrm{MR}(bR_2)(R^{-1})^2 \pmod N \\
&\equiv aR_2R^{-1} \cdot bR_2R^{-1} \cdot (R^{-1})^2 \pmod N \\
&\equiv aR \cdot bR \cdot (R^{-1})^2 \pmod N \\
&\equiv ab \pmod N
\end{aligned}
$$

である．$0 \leqslant \mathrm{MR}(C) < N$ なので，$\mathrm{MR}(C) = ab \% N$ である． □

Corollary 2.1. $R_2 = R^2 \% N$ とおく．$0 \leqslant a < N$, $0 \leqslant b < N, 0 \leqslant c < N$ について，$A = \mathrm{MR}(aR_2)$, $B = \mathrm{MR}(bR_2), C = \mathrm{MR}(cR_2)$ とし，$A' = \mathrm{MR}(AB)$, $D = \mathrm{MR}(A'C)$ とおくと，$\mathrm{MR}(D) = abc \% N$ である．

Proof. まず，$0 \leqslant aR_2 < NR, 0 \leqslant bR_2 < NR, 0 \leqslant cR_2 < NR, 0 \leqslant AB < NR, 0 \leqslant A'C < NR, 0 \leqslant D < NR$ である．次に，

$$
\begin{aligned}
\mathrm{MR}(D) &\equiv DR^{-1} \pmod N \\
&\equiv \mathrm{MR}(A'C)R^{-1} \pmod N \\
&\equiv A'C(R^{-1})^2 \pmod N \\
&\equiv \mathrm{MR}(AB)C(R^{-1})^2 \pmod N \\
&\equiv ABC(R^{-1})^3 \pmod N \\
&\equiv aR_2 \cdot bR_2 \cdot cR_2 \cdot (R^{-1})^6 \pmod N \\
&\equiv abc \pmod N
\end{aligned}
$$

である．$0 \leqslant \mathrm{MR}(D) < N$ なので, $\mathrm{MR}(D) = abc \% N$ である． □

Corollary 2.2. $R_2 = R^2 \% N$ とおく．$0 \leqslant a < N$, $k \geqslant 0$ について，$A_1 = \mathrm{MR}(aR_2), A_l = \mathrm{MR}(A_1A_{l-1})$, $l = 2, 3, \ldots, k$ とおくと，$\mathrm{MR}(A_k) = a^k \% N$ である．

Proof. $0 \leqslant aR_2 < NR$, $0 \leqslant A_1A_{l-1} < NR$, $l = 2, 3, \ldots, k$ である．

$1 \leqslant l \leqslant k$ について，$A_l \equiv A_1^l(R^{-1})^{l-1} \pmod N$ を示す．$A_1 \equiv A_1^1(R^{-1})^0 \pmod N$ より，$l = 1$ のとき成り立つ．$2 \leqslant l \leqslant k$ のとき，帰納法の仮定より，

$$
\begin{aligned}
A_l &\equiv \mathrm{MR}(A_1A_{l-1}) \pmod N \\
&\equiv A_1A_{l-1}R^{-1} \pmod N \\
&\equiv A_1 \cdot (A_1^{l-1})(R^{-1})^{l-2}R^{-1} \pmod N \\
&\equiv A_1^l(R^{-1})^{l-1} \pmod N
\end{aligned}
$$

である．

したがって，

$$
\begin{aligned}
\mathrm{MR}(A_k) &\equiv A_kR^{-1} \pmod N \\
&\equiv A_1^l(R^{-1})^l \pmod N \\
&\equiv \mathrm{MR}(aR_2)^l(R^{-1})^l \pmod N \\
&\equiv (aR_2R^{-1})^l(R^{-1})^l \pmod N \\
&\equiv a^l \pmod N
\end{aligned}
$$

である．また，$0 \leqslant \mathrm{MR}(A_k) < N$ より，$\mathrm{MR}(A_k) = a^l \% N$ である． □

Lemma 2.3. $R = 2^m$ とする．

$$
\mathrm{MR}(T) = \begin{cases}
(T + (TN' \,\&\, (R-1))N) \ll m, & (T + (TN' \,\&\, (R-1))N) \ll m < N, \\
(T + (TN' \,\&\, (R-1))N) \ll m - N, & (T + (TN' \,\&\, (R-1))N) \ll m \geqslant N
\end{cases}
$$

である．ただし，& はビット積，« は左シフト演算を表す．

Proof. 明らか． □