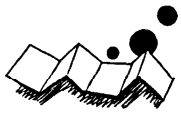
解　説

3. 光情報処理システム



3.5 光剰余演算†

石　原　聰††

1. はじめに

「ここに碁石がいくつかあります．3人で分けると2個余り，4人では3個，7人では4個余りますが，5人ではぴったり割り切れます．さて，全部でいくつあるのでしょう？」子供の頃こんな問題を出された覚えのある方があるかもしれない．ある決まった数で割ったときの「余り」に着目する「剰余演算」は決して新しい概念ではなく，遡れば1世紀の中国で上のような問題が解かれているとのことである．

この剰余演算を数値の計算に利用しようという考えは最近でも少なくないが，コンピュータへの応用についてもすでに1950年代から60年代にかけて多くの試みがある[1]．この情報処理誌においても，第1巻に，高橋らの論文[2]を見ることができる．

しかしながら，剰余演算と光を積極的に結びつけようとする最近の研究が始まったのは1975年[3]である．本稿では，このような光を用いた剰余演算についての基礎的な考え方をまとめ，最近の研究動向を概観する．

以下，**2.**では，剰余演算についてまったく予備知識のないことを前提にして基礎的な事項を説明する[4]．整数論，合同式の演算，あるいは時計算などについてご存知の方は**2.**を読み飛ばして**3.**に進んでいただきたい．**3.**では，光剰余演算に関する最近のさまざまな研究を紹介する．

2. 剰余演算

本章では，剰余数系，そこでの四則演算，および一般の数系との間の変換法など，剰余演算の基本的事項とそれらに基づく特徴について述べる．

2.1 剰余数系

剰余数系（residue number system）は，法（modulus）と呼ばれるN個の互いに素な整数 $m_1, m_2, \cdots, m_N$ の上に成立している．すなわち，任意の m_i と m_j は共役数を持たない．ある法 $m_i (i=1,2,\cdots,N)$ に対する，任意の整数Xの剰余（residue）は，Xを m_i で除したときの「余り」のうち最小の非負数 $Rm_i(X)$ によって，（1）式，（2）式のように定義される．

$$Rm_i(X)=X-k\cdot m_i \qquad (1)$$

$$0\leqq Rm_i(X)<m_i \qquad (2)$$

ここで，kは（2）式が満足されるように選ばれた整数であるが，剰余数系ではこのkの値自体は意味を持たない．この剰余 $Rm_i(X)$ を，以下では，必要に応じて，$\mathrm{mod}\,(X, m_i)$ あるいは，混同の生じない場合は単に Rm_i などと表す．

$$M=\prod_{i=1}^{N} m_i=m_1\times m_2\times\cdots\times m_N \qquad (3)$$

とすると，連続するM個の整数の1つ1つに対して，N個の剰余の組

$$\{Rm_1, Rm_2, \cdots, Rm_N\} \qquad (4)$$

が一対一対応で定まる．（この対応関係を⟷で表現する．）これらの $Rm_i (i=1,2,\cdots,N)$ は剰余数系における各「桁」の値とみなすこともできる．

［例 1］ 本稿の数値例では，$N=4$, $m_1=3$, $m_2=4$, $m_3=5$, $m_4=7$ という系を用いることにする．

この系では，（3）式より $M=420$ であるので，たとえば 0～419，あるいは −210～209 のような連続する420個の整数を一意に表現できる．

$X=95$ について，（1），（2）式を適用すれば，

$\{Rm_1, Rm_2, Rm_3, Rm_4\} = \{2, 3, 0, 4\}$

がただちに得られる．

2.2 四則演算

2.1で定義した剰余数系における，基本的な四則演算について述べる．

（a） 加　算

2つの整数 X, Y の，剰余数系における加算は，N

† Optical Residue Arithmetic by Satoshi ISHIHARA (Electrotechnical Laboratory).

†† 電子技術総合研究所

個の法の各々に対して和を求めることによって成立する．和が法の値以上になったときは，和の剰余をあらためて和とする．すなわち，2数 X, Y の（剰余演算の意味での）和 $S=X+Y$ の剰余数系における表現のうち，i 番目の法 m_i に対する剰余は，

$$Rm_i(S)=\mathrm{mod}\,(\mathrm{mod}\,(X, m_i)+\mathrm{mod}\,(Y, m_i), m_i) \quad (5)$$

で表される．

[例 2]　$X=95$ と $Y=173$ の和を求める．

$173\leftrightarrow\{2, 1, 3, 5\}$ であるから，例1で求めた $X=95\leftrightarrow\{2, 3, 0, 4\}$ と，項別に剰余加算を行うと，$\{2+2, 1+3, 3+0, 5+4\}=\{1, 0, 3, 2\}$ を得る．これは，$S=X+Y=268$ に対する剰余数表現 $\{1, 0, 3, 2\}$ と一致している．

このように，剰余数系では，加算は各項ごとに独立に行えばよい．通常，われわれが使用している数系（10進法，2進法など）* では桁上り（carry）が生じることがあるので，各桁ごとに独立に加算できないが，それと対照的とも言える．

なお，剰余数系における（ある法に対する）加算に対して，通常の「九九」と同様の表を作ることができる．例として，法が4の場合の加算表を**表-1** に示す．この表で明らかなように循環的（cyclic）になるのが，剰余数系における加算表の特徴である．

（b）減　　算

剰余数系における2数 X, Y の差 $D=X-Y$ の，法 m_i に対する剰余は，加算の場合と同様に，

$$Rm_i(D)=\mathrm{mod}\,(\mathrm{mod}\,(X, m_i)-\mathrm{mod}\,(Y, m_i), m_i) \quad (6)$$

となる．もちろん，加算の場合と同様の（循環的な）減算表も作成できる．(6)式は，

$$Rm_i(D)=\mathrm{mod}\,(\mathrm{mod}\,(X, m_i)+(m_i-\mathrm{mod}\,(Y, m_i)), m_i) \quad (7)$$

とも変形できる．すなわち，減数 Y の剰余 $\mathrm{mod}\,(Y, m_i)$ の，法 m_i に対する補数（加法的逆数（additive inverse）とも言う）$m_i-\mathrm{mod}\,(Y, m_i)$ を被減数に加えることによっても，差が求まる．この補数 $m_i-\mathrm{mod}\,(Y, m_i)$ は，$-Y$ の表現にほかならない．

（c）乗　　算

剰余数系においては，2数 X, Y の積 $P=X\cdot Y$ を求める乗算についても，加算・減算と同様に(8)式のように項別に（すなわち，各々の法に対して独立に）乗算を行えばよい．

$$Rm_i(P)=\mathrm{mod}\,(\mathrm{mod}\,(X, m_i)\cdot\mathrm{mod}\,(Y, m_i), m_i) \quad (8)$$

当然，乗算に対しても「乗算表」を作ることができるが，一般には加減算の場合のように循環性は見られない*．**表-2** に，法が4の場合の乗算表を示す．

[例 3]　$X=16$ と $Y=22$ の乗算．

X と Y の剰余数表現 $\{1, 0, 1, 2\}$ と $\{1, 2, 2, 1\}$ の「項別」乗算の結果 $\{1\times1, 0\times2, 1\times2, 2\times1\}=\{1, 0, 2, 2\}$ を得るが，これは16と22の積352に対応する．

このように，乗算を加減算と同じ手間で実行できることが，この剰余数系の特長の1つである．

（d）除　　算

剰余数系は整数に対して定義されているので，2数の商を一般的に剰余数で表現できるとは限らない．そこで，除算を乗算の逆演算としてとらえ，除算 X/Y に対しては，ちょうど $Q\cdot Y=X$ となるような数 Q が存在する場合に，商として Q が定義できるものとしよう．

例として法が4の場合の除算を考える．たとえば，$2\div0$ の商は，$Q\times0=2$ となるような数 Q が表-2 に存在しないから，存在しない．これはわれわれが日常使っている数系と同様である．$2\div1$ は，$Q\times1=2$ を満たす数 $Q=2$ が 表-2 中に見つかるので，商が2と

表-1　剰余数の加算表の例 $R_4(X)+R_4(Y)$

$R_4(X)$ \ $R_4(Y)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

表-2　剰余数の乗算表の例 $R_4(X)\cdot R_4(Y)$

$R_4(X)$ \ $R_4(Y)$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

* よく知られているように，たとえば l 進法（l は正の整数）において，整数 X は，$\pm\sum_k a_k\cdot l^k\ (0\leq a_k<l)$ で表現できる．

* 法が素数の場合には，あらかじめ表の配列を置換えることによって（0の項を除いて）循環的な表を作ることができる．

表-3 剰余数の除算表の例 $R_4(X)/R_4(Y)$

$R_4(X)$ \ $R_4(Y)$	0	1	2	3
0	*	0	0	0
1	*	1	*	3
2	*	2	1, 3	2
3	*	3	*	1

*：不定または不能

表-4 剰余数の乗算表の例 $R_5(X)/R_5(Y)$

$R_5(X)$ \ $R_5(Y)$	0	1	2	3	4
0	*	0	0	0	0
1	*	1	3	2	4
2	*	2	1	4	3
3	*	3	4	1	2
4	*	4	2	3	1

*：不定または不能

なる．これも，1で割ったときの商は被除数と一致するというわれわれの常識から外れない．次に $2\div 2$ であるが，$Q\times 2=2$ となる値は，表-2を見ると，$Q=1$ のほかに $Q=3$ が存在する．つまり，この場合，商は一意に定まらない．最後に $2\div 3$ については，同様にして商2を得る．これらをまとめた，法4に対する除算表を表-3に示す．表中の＊は，商が存在しない場合を表す．

一般に，法が素数の場合は，(除数が0でないときに) 商は一意に定まる*．法が5の場合の除算表を表-4に示す．

$$\mathrm{mod}\,(X\cdot Y, m_i)=1 \qquad (9)$$

が成立するとき，X を，法 m_i に対する Y の乗法的逆数 (multiplicative inverse) と呼び，

$$X=\left|\frac{1}{Y}\right|_{m_i} \qquad (10)$$

と書く．明らかな場合は，m_i を略すこともある．

[例 4] 表-4 より，$\left|\frac{1}{2}\right|_5=3$，$\left|\frac{1}{4}\right|_5=4$

除算の実行にあたっては，除数に乗法的逆数が存在するときに限って，この逆数と被除数との積を求めることによって商を得ることができる．すなわち，

$$Rm_i(Q)=\mathrm{mod}\,(\mathrm{mod}\,(X, m_i)\cdot\left|\frac{1}{Y}\right|_{m_i}, m_i) \qquad (11)$$

[例 5] $323\leftrightarrow\{2,3,3,1\}$ を $19\leftrightarrow\{1,3,4,5\}$ で除する．$\{1,3,4,5\}$ の乗法的逆数はすべて存在して，$\{1,3,4,3\}$ となる．これを用いて，

$$\{2\times 1, 3\times 3, 3\times 4, 1\times 3\}=\{2,1,2,3\}\leftrightarrow 17$$

しかし，例3の逆演算 $352\div 16$，$352\div 22$ を行おうとしても，法4に対する除数の乗法的逆数が存在しないので，商を得ることは不可能である．

(e) 複 合 演 算

(a)～(d)において，剰余数系では，一般に，

$$Rm_i(X*Y)=\mathrm{mod}\,(\mathrm{mod}\,(X, m_i) *\mathrm{mod}\,(Y, m_i), m_i) \qquad (12)$$

が成立することが示された．ここで，＊は加減乗算を表す．

これを拡張することによって，有限個の加減乗算から成る複合的な演算（多項式演算，行列演算など）についても，演算は個々の法ごとに独立に実行すればよいことがわかる．

2.3 剰余数系からの逆変換

われわれが通常使用している数系から剰余数系への変換についてはすでに2.1で述べたが，実際にはこの逆変換法も必要である．このための変換法を一般的に与えるのが「中国剰余定理」であり，さらに一層実用的な方法が混合基数系への変換である．

(a) 中国剰余定理

互いに素である法 $m_1, m_2, \cdots\cdots, m_N$ の上に成立している剰余数系において，整数 X が $\{Rm_1, Rm_2, \cdots, Rm_N\}$ で表されるとき，(13)式が成立する．

$$\mathrm{mod}\,(X, M)=\mathrm{mod}\left(\sum_{i=1}^{N}\hat{m}_i\cdot\left|\frac{1}{\hat{m}_i}\right|_{m_i}\cdot Rm_i, M\right) \qquad (13)$$

ここで，M は(3)式で定義した値，また

$$\hat{m}_i=M/m_i=\prod_{\substack{j=1\\ j\neq i}}^{N} m_j \qquad (i=1,2,\cdots,N) \qquad (14)$$

である．これを中国剰余定理 (Chinese remainder theorem) と呼ぶ．この定理によって，任意の剰余の組 $\{Rm_1, Rm_2, \cdots, Rm_N\}$ から X への変換が保証される．

[例 6] 本稿で用いている例，$m_1=3, m_2=4, m_3=5, m_4=7$ の場合の逆変換を考える．$M=420$，$\hat{m}_1=140$，$\hat{m}_2=105$，$\hat{m}_3=84$，$\hat{m}_4=60$ であるので，

* 読者は各自でチェックされたい．なお，これは，素数に関する剰余類の性質から導かれる．

$\left|\frac{1}{\hat{m}_1}\right|_{m_1}=2$, $\left|\frac{1}{\hat{m}_2}\right|_{m_2}=1$, $\left|\frac{1}{\hat{m}_3}\right|_{m_3}=4$, $\left|\frac{1}{\hat{m}_4}\right|_{m_4}=2$

となり，$0\leqq X<M$ とすると，(13)式は，

$X=\mathrm{mod}\,(280\cdot R_3+105\cdot R_4+336\cdot R_5+120\cdot R_7, 420)$

で与えられる．

たとえば，例1で得られた剰余数 {2, 3, 0, 4} の値をこの式に代入すると，$X=\mathrm{mod}\,(1355, 420)=95$ が得られる*．

このように，中国剰余定理は剰余数系から，われわれになじみの深い数系への一般的変換法を与えるが，例からも明らかなように通常の数系で多くの演算を必要とし，実用的とは言えない．より実際的な方法としては，次に示す混合基数系への変換がある．

(b) 混合基数系への変換

(a)の場合と同様の剰余数系において，Xを

$$X=\sum_{i=1}\left(a_{N-i+1}\cdot\prod_{j=1}^{N-i}m_j\right)+a_1 \qquad (15)$$

の形で表現すると，この式で定められる a_i の組

$$\langle a_N, a_{N-1}, \cdots, a_1\rangle \qquad (16)$$

は X と一対一対応する．ここで，$a_i(i=1, 2, \cdots, N)$ は，

$$0\leqq a_i<m_i \qquad (17)$$

を満たす整数である．(15)式の表現を，Xの混合基数系 (mixed radix number system) 表現という．

剰余数系表現 $\{Rm_1, Rm_2, \cdots, Rm_N\}$ から，混合基数系表現 $\langle a_N, a_{N-1}, \cdots, a_1\rangle$ を求める具体的な手法は次のようになる．まず，a_1 は，(15)式の両辺を m_1 で割ったときの余りから求められる．すなわち，左辺を m_1 で割った余りは(1)～(2)式の定義より，$\mathrm{mod}\,(X, m_1)=Rm_1$．一方，右辺の $(N-1)$ 個のカッコ内の項はすべて m_1 という因子を持っているので m_1 で割り切れ，残りは a_1 となるので余りは a_1 となり，結局，$a_1=Rm_1$ を得る．次に，a_2 については，まず(15)式の両辺から $Rm_1=a_1$ を差し引き，その結果を m_2 で割った余りから求める．左辺は，$\mathrm{mod}\,(X-Rm_1, m_2)$，右辺は a_2 となるので，$a_2=\mathrm{mod}\,(X-Rm_1, m_2)$ を得る．a_3 以降についても同様の方法で求められる．

[例 7] {2, 3, 0, 4} の混合基数系表現への変換．

(15)式から，

$$X=a_4\cdot(m_1\cdot m_2\cdot m_3)+a_3(m_1\cdot m_2)+a_2\cdot m_1+a_1$$
$$=60a_4+12a_3+3a_2+a_1 \qquad (18)$$

を満たす $\langle a_4, a_3, a_2, a_1\rangle$ を求めることになる．具体的な手法を**図-1**に示す．表中の減算や除算も剰余演算の意味で実行される．たとえば，除算は乗法的逆数との乗算による．得られた $\langle a_4, a_3, a_2, a_1\rangle=\langle 1, 2, 3, 4\rangle$ を(18)式に代入し，95が得られる．

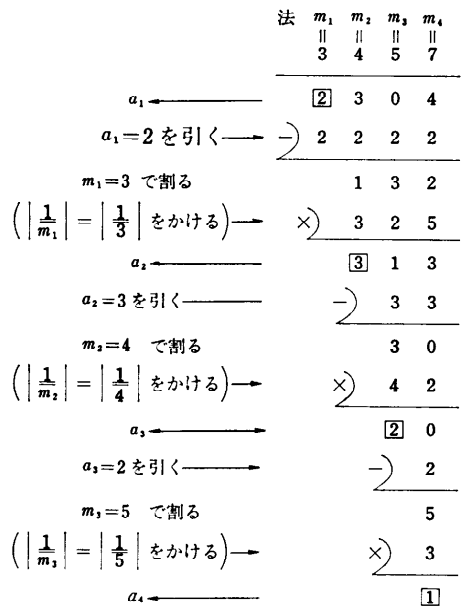


図-1 混合基数系への変換の例

{2, 3, 0, 4} より

$X=a_4\cdot(m_1\cdot m_2\cdot m_3)+a_3(m_1\cdot m_2)+a_2\cdot m_1+a_1$

$=1\times(3\times4\times5)+2\times(3\times4)+3\times3+2$

$=95$

を得る．

なお，剰余数系と通常われわれが使用している系との間の変換は，すべての演算の最初と最後に1回ずつ行えばよいことを最後に指摘しておきたい．

3. 光を用いた剰余演算

剰余演算の一つの特徴が，演算を(キャリーなしに)並列で，したがって高速に実行できる可能性をもつことである点は**2.2**(a)で述べた．以下で述べるように光は少なくとも原理的に剰余演算自体あるいは通常の数と剰余数の間の変換に適している．これは光がもつ並列処理性による．

また(3)式からも明らかなように剰余数系では小さなダイナミックレンジの素子を用いて大きな数を取り扱うことができる．このことは，せいぜい 10^3 程度のダイナミックレンジしかとれないアナログ演算から，精度の向上をはかってディジタル演算を指向している光情報処理[6]にとって大きな魅力である．

* 本文冒頭の碁石の問題の解に相当している．

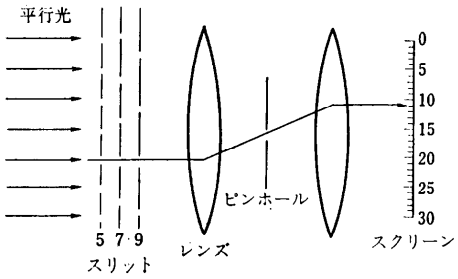


図-2　周期の異なるスリットを用いた光剰余演算[3]

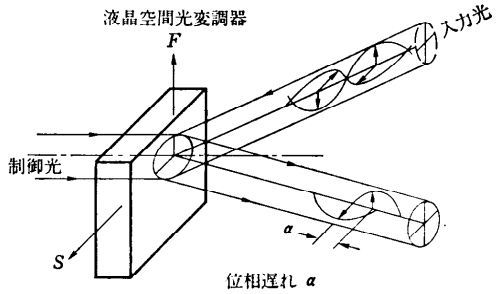


図-3　光の偏波状態を用いた剰余数表現[10]

はじめにも述べたように，剰余算法自体やその応用については多くの研究があるが，光学的な実現法についての最近の活発な研究のきっかけを作ったのは，Huang による提案[13]であると思われる*．彼は，**図-2** のように，法 $m_i(i=1,2,\cdots,N)$ の同期を持つ N 個のスリットを並べ，それらをそれぞれ剰余の値 Rm_i ずつずらしたときに，そのすべてを通過する光によって，剰余数との間の変換・逆変換，加算などが実現できるとした．その後，彼の属する Stanford 大学では，光学的な手法を用いた剰余演算に関する研究が系統的に行われたが，そこでは，その後の光剰余演算の研究の基本的事項のほとんどが扱われているので，以下ではその成果を基に光剰余演算について考察し[8]，さらにその後現在に至るまでの研究開発の成果を網羅的に紹介する．

3.1 剰余数の光学的表現

（a） 空間的な方法

剰余演算を光学的に実現するためには，ある光学的な物理量によって剰余数を表現する必要がある．最も実際的な方法は，法が m である剰余数に対しては空間的に m 個の場所を定め，そのいずれに光があるかによって，$0,1,\cdots,m-1$ のいずれかの値を表すというコーディング法である．この方式は実現も容易であるし，ノイズにも強いので最も多く使用されている．

空間的な場所を節約するためには剰余数の値を2進表現し，その各桁が1であるかないかによってそれぞれに対応する場所に光を割り当てるという方法をとればよい．この場合，必要な場所の個数は $[\log_2 m]$ 個となる．ここに，$[x]$ は，x の小数部分を切り上げた整数である．

（b） 時間的な方法

同様に，時間的な表現も考えうる[9]．上の2つの例をそのまま置き換えれば，一種のパルス位置変調 (PPM)，パルス符号変調 (PCM) とも言えよう．

（c） 周期的な光学量による方法

2. で述べたように，**剰余演算では循環的な演算が有用となる．よく知られているように，光の位相や偏波面（の傾き）は，ある一定量 (360°) だけ変化すると元と同じ性質を示す周期性をもっているので，剰余数の表現に適している．** Ohio 州立大の Collins, Jr. らは，法が m の場合，お互いに $(360/m)°$ ずつ傾いた楕円偏波主軸の傾きで，0から $(m-1)$ までの剰余数を表現するシステムで，**図-3** のような液晶空間光変調器を用いた加算・乗算法を提案した[10]．この変調器は，その各点に入った光の偏波面を，同じ点に到達する別の制御光の大小に応じて2つの直線偏波モード間に位相遅れ α を与え，その結果ある一定角 ϕ だけ回転して反射する機能をもっている．$\phi=(360/m)\cdot j°$ ならば，$+j$ の加算が実行されるし，光学系を工夫して，同じ点で続けて k 回の多重反射を行わせれば，$\times k$ の乗算が実行される．

3.2 剰余演算とマップ

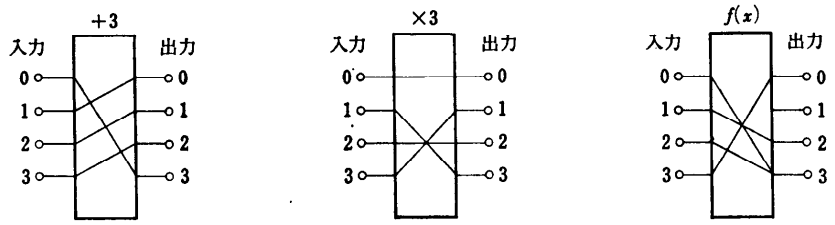
（a） マ ッ プ

剰余数系における加減算・乗算や多項式の計算は，表-1～4 のように，表の形にまとめられる．この表の一列だけを抜き出してみると，m 個の入力に対する出力の対応を表すことになるので，このような対応関係を「マップ」と呼ぶ．**図-4** にマップの例を示す．このようなマップは，**3.1**（a）で述べた，光の空間的な位置によって数を表現する場合には，基本的な素子の実体的な概念にも対応することになるので特に有用である．

加減算の場合や，素数を法とする場合の（0以外の数との）乗算では，1つの出力が1つの入力にだけ対応しているような「置換マップ」となる．

加減算・乗算などのように複数入力（被演算数）に

* 文献によれば，すでに1933年に，「光電的数篩 (photo-electric number sieve)」なるものが作られている[9]．この名称から，大体の構造がおわかりになるのではないだろうか？



（a） 加算（+3）　（b） 乗算（×3）　（c） 多項式の計算（$f(x)=x^3-2x+3$）

図-4 固定マップの例（法 $m=4$ の場合）

出力（演算結果）が対応する場合は，1つの入力を変えたときにこれに対応してマップの「結線」を変えることによって演算を実行できる．このようなマップを「可変マップ」と呼ぶ．

（b） マップの光学的実現法

3.1(a) で述べたように，光の空間的な位置によって入出力の数値を表している場合，マップの光学的実現法としては，空間内を直進する光線を対象にすれば，反射・屈折・回折などの利用が考えられる．より直接的な方法としては，光ファイバ，光 IC などの光導波路が利用できる．

3.3 循環可変マップとその光学的構成例

剰余演算における加減算，及び法が素数である場合の乗算（2.2(c)脚注参照）は循環的にでき，そのような演算に対するマップは「循環マップ」となる．循環的な演算のための循環可変マップは，「任意の循環的置換は，2つの部分的な循環的置換と逆転置換の積で構成できる」という性質を使うと，簡単に構成できる．

図-5 に，このような考え方の，循環可変マップへの適用例を示す．この例は，法 $m_i=4$ の場合の加算用可変マップの実行例であり，入力（加数）は0～3のいずれかをとる空間的な表現である．一方，被加数はその剰余数の2進表現値が1のとき，1桁目は上のブロック，2桁目は下のブロックに制御信号を送る．各ブロック内には，外部から制御信号が入ったとき，反射状態になる M_+ と透過状態 M_- になる可制御鏡があるので，上下のブロックで各々，制御信号に応じて $+2^0=+1$，$+2^1=+2$ が実行され，結局 $m_i=4$ の任意の加算が行われる．

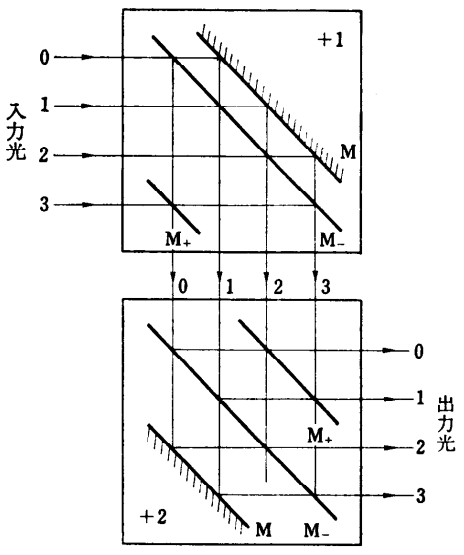


図-5 循環的な演算のための可変マップの例[11]
可制御鏡を用いた $m=4$ の可変加算マップ

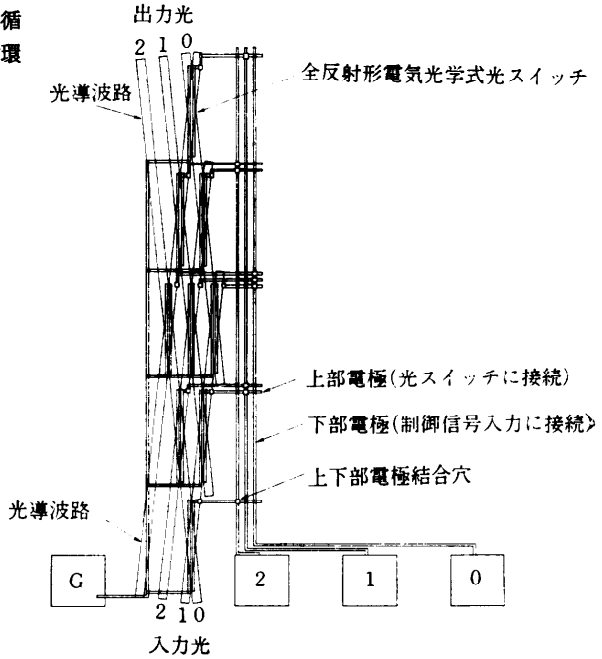


図-6 全反射形電気光学式光スイッチアレイによる可変マップ（$m=3$）[11]

3.4 光 IC による剰余演算

（a） 光 IC スイッチによる可変マップ

3.2(b) でも触れたように，光剰余演算の実現法としては，光導波路を用いた光 IC 形スイッチによる可変マップの利用が有望である[7]．

この方式について Boeing 社の Polky と Miller が詳細設計を行った．$LiNbO_3$ 基板上の全反射形電気光学式光スイッチアレイの構成例[11]を図-6 に示す．この基本素子を用いて，23 ビットの精度で毎秒 2.5×10^9 演算の実行が可能であると述べている[12]．

（b） 光制御形可変マップ

図-6 からもわかるように，このようなタイプの光導波路素子は制御信号用の電極を基板上に設ける必要があるため，特に法の値が大きくなるにつれてその製作が困難になり，しかも電極間の電気的干渉などが増す．この問題を解決するため，電総研の石原らは，光-光制御形導波路素子を用いた光 IC アレイ演算器によって，外部からの制御光で可変マップを制御する方式を提案している[13]．このような光制御方式には，制御光パターンを変えることなく単に横に移動するだけで循環マップの制御ができる（図-7）など，システムの設計を容易にする可能性もある．

（c） 汎用マップ・モジュール

ERIM（ミシガン環境研）の Cindrich らは，光 IC 形の光スイッチを用いて 1 つの素子で加減乗（除）算ができる汎用マップ・モジュール（図-8）について，検討を行った[14]．

3.5 剰余数への変換方式

（a） 2 進数表示からの変換

通常の数を剰余数に変換するには，必ずしも 2.1 で述べたように除算を実行して「余り」を求める必要はない．たとえば，通常の I 桁の 2 進数で表現されている数

$$X=\sum_{i=1}^{I} x_i\cdot 2^{i-1}$$

$(x_i=0$ または $1)$ (19)

の剰余数（法 m）への変換を考える．

$$R_m(X)=\sum_{i=1}^{I} x_i\cdot R_m(2^{i-1}) \qquad (20)$$

であるので，i 番目の x_i が 1 であるときにだけ定数 $R_m(2^{i-1})$ を加えていけばよい．したがって，図-5 の形の循環可変マップを直列的に 図-9 のように接続してできる加算器によって，剰余数への変換ができる．入力が 10 進数表現であっても，同様の手法が利用できる．

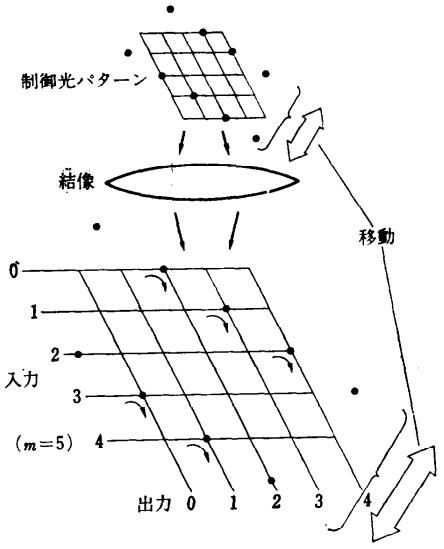


図-7 光-光制御形導波路素子で構成される光 IC アレイ演算器を用いた可変循環マップ $(m=5)$[13]

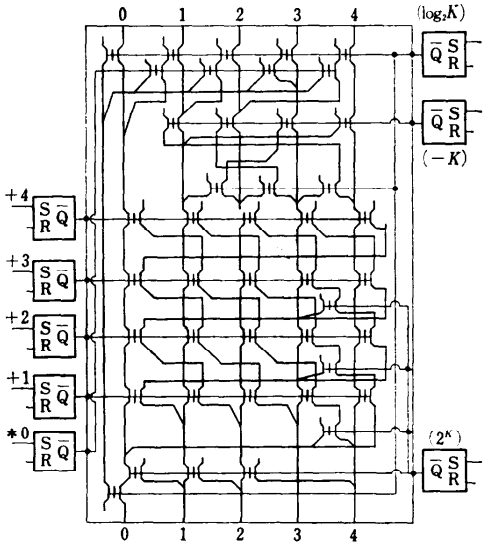


図-8 光 IC 形汎用マップ・モジュール $(m=5)$[14]

入力がアナログ的な量である場合に対しては，次のような方式が提案されている．

（b） 万華鏡方式

Science Applications 社の Horrigan らは，図-10 に示す，万華鏡のような光学系によって，直線状の点が周期的に再配置されることを利用した[15]．

（c） 光学的相関の利用

Carnegie-Mellon 大の Psaltis らは，空間的な相

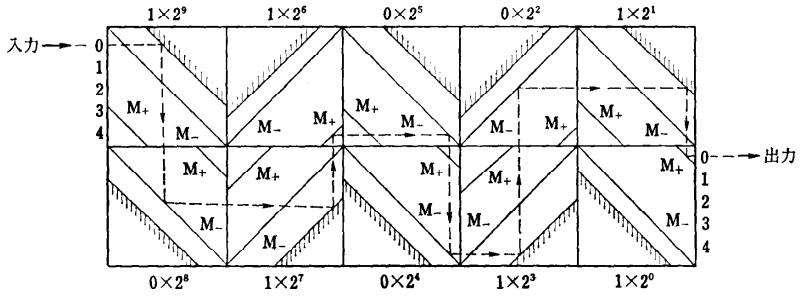


図-9 2進数入力に対する剰余直列加算器 ($m=5$)[11]

外部からの入力が1のとき，可制御鏡 M_+ は反射，M_- は透過；外部からの入力が0のとき，可制御鏡 M_+ は透過，M_- は反射となる．この例では，$0+\mathrm{mod}(715,5)=0$ を実行している．715は2進数表示で 1011001011 である．

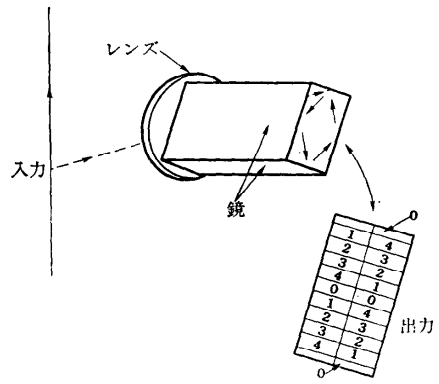


図-10 万華鏡方式による剰余数への変換 ($m=5$)[15]

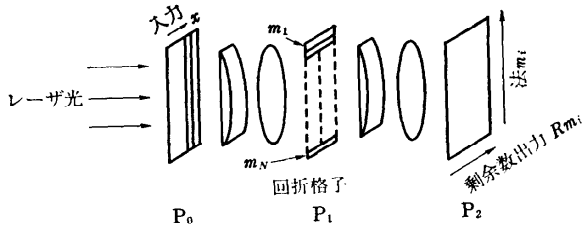


図-11 空間積分形光相関器を用いた，剰余数への変換[16]

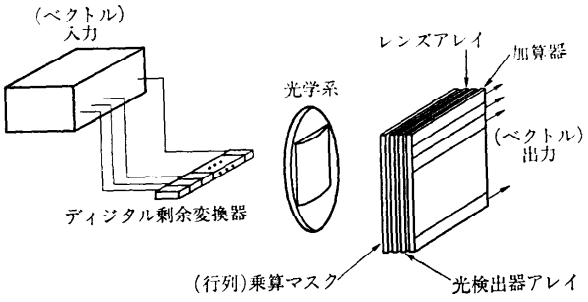


図-12 光剰余行列ベクトル演算器[7]

関演算を利用した，剰余数への変換と逆変換法を提案した[16]．**図-11** の入力面 P_0 の入力 X に比例する空間座標点から出た光は，P_0 のフーリエ変換面 P_1 に置かれた法 m_i に比例する空間周波数をもつ矩形状回折格子によって，回折され出力面 P_2 では，原点から X に比例した量だけ位置ずれした，m_i に比例した間隔で並ぶ多数の点に結像する．P_2 面に適当な窓を置くことによって，変換後の剰余数表現が得られる．図-11 のように，縦方向の空間を利用することによって，同一入力 X に対して同時に多数の m_i についての変換が可能となる．逆変換については，この図-11 の逆方向の変換を行い，P_1 面ですべての m_i について出力が現れるのを検出する．

さらに，Psaltis らは，剰余数への変換系のダイナミックレンジ（Mに対応）を大きくとるため，時間積分形の相関器構成も示している[9]．この場合，入力は時間的に位置を変調した単パルスで与えられるが，出力は空間的な位置となる．周波数の異なる超音波を多重化することによって，複数の法 m_i に対する同時変換が可能となる．

3.6 光剰余演算による数値演算システム

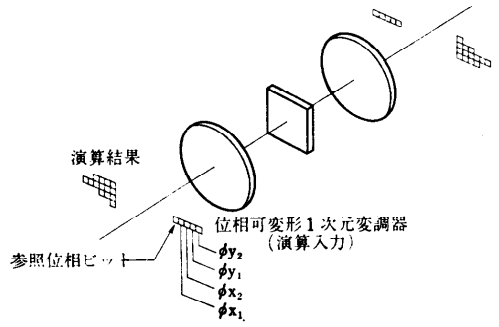
以上に述べたような基本的素子を組み合わせることによって，加減乗算から成る演算，たとえば，行列とベクトルの乗算器を構成できる．**図-12** にその一例[7]を示す．

以下では，光剰余演算を用いた数値演算の方式をいくつか紹介する．

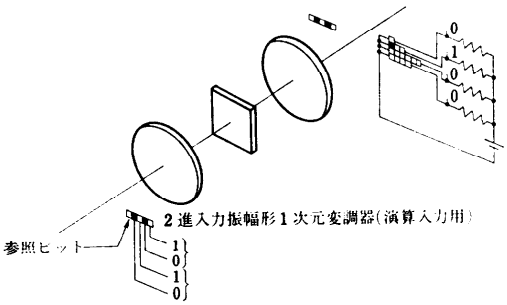
（a） テーブル・ルックアップ式演算器

一般に2つの数の間の演算によって1つの結果が得られる場合，これを1つの「表(table)」にまとめることができる（表-1～4

は，取り扱われる数の範囲こそ限られているが，そのような「表」の例と言える）．実際に2つの「入力」が与えられたときには，「表」のどこに対応する「結果」が記されているかを「ひく（look up）」必要がある．最も単純なのは，入力に対応するアドレスごとに答を記録する方法であるが，容易に想像できるように「表」が膨大になる．逆に，「結果」で分類した「表」を作ってその内容には入力の組み合わせを記録しておき（たとえば，6というラベルの所には，1×6, 2×3, 3×2, 6×1 を記録しておく），演算の際には「入力」とこの記録内容を比較して『一致』した場合には，対応するラベルを「結果」としようという一種の連想記憶方式を用いれば，「表」のサイズをかなり小さくできる．Georgia 工科大の Guest らは，光学的なホログラフィによる光の振幅の複素的加算を用いて，上述の『一致』の検出を並列に一度にでき，しかもその「結果」をただちに出せるという方式を提案した[17]．**図-13** に，そのような「表」に対応するホログラムの作製方法とこれを用いた演算方法の一方式を示す．



（a） ホログラフィによる「表」の作製



（b） 2数の乗算の例

図-13 ホログラフィックなテーブルルックアップ方式を用いた光数値演算[17]

このような方式で使用する数値に対して剰余数表現を用いれば，「表」の大きさを著しく減らすことができる[18]．たとえば，17ビットの2数の乗算に対して単純な2進数表現を用いると 2.7×10^{11} のホログラムが必要となり実現の可能性は小さいが，対象とする数値を，4, 5, 7, 9, 11, 13を法とする（2進数表示の）剰余数で表現すれば，必要なホログラム数はわずか 694 となる．この数をさらに小さくする努力も続けられているが[19]，p を素数とする時 p^n の形をもつ法を選ぶことが有効であり，たとえば $p=3$ の場合の光学的な実現法が報告されている[20]．

（b） 光・電子複合式行列乗算器

新潟大の安東らは，剰余算法を用いた，行列の乗算について，多重エンボスホログラムアレイ[21]，LED マトリクスアレイ[22]を利用したユニークな方式（**図-14**）を提案している．

ここで次数 n の2つの正方行列 A, B の積 C を求めることを考える．各々の要素 a_{ik}, b_{kj}, c_{ij} は m を法とする剰余数で表現される．入力 a_{ik}, b_{kj} は，LED

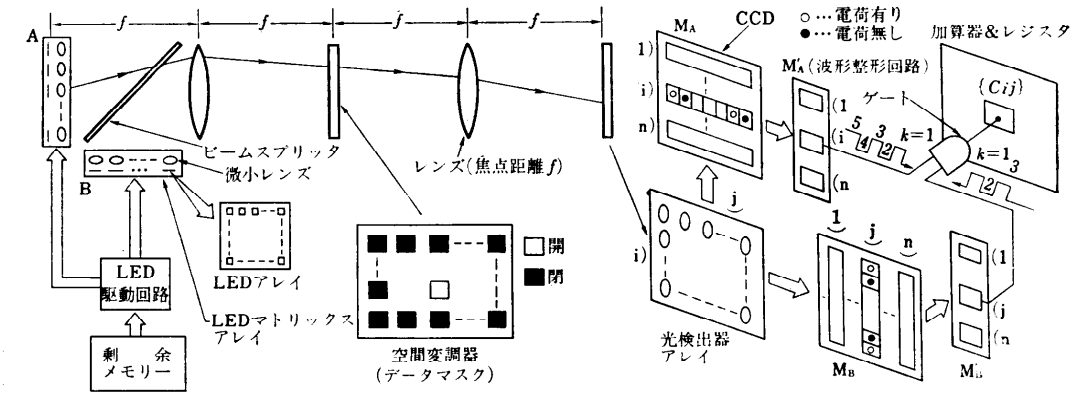


図-14 剰余演算を利用した光電子複合式行列乗算器[23]

マトリクスアレイの発光位置で表されている．$c_{ij}=\sum_k a_{ik}b_{kj}$ を求めるためには m を法とする乗算表（例，表-2）のある $a=Rm(X)$, $b=Rm(Y)$ の組み合わせについて，$k=1$ から n まで $a_{ik}=a$ でかつ $b_{kj}=b$ となる (a_{ik}, b_{kj}) の組を検索し，1組検索するごとに値 $(a\cdot b)$ を剰余的に加算していく（検索された組数を l_{ijab} とする）．この加算を乗算表のすべての（非ゼロの）要素について（表-2の場合は，8通り）行えば，結果の $\sum_{a=1}^{m-1}\sum_{b=1}^{m-1} l_{ijab}\cdot(a\cdot b)$ が c_{ij} に等しくなる．$a_{ik}=a, b_{kj}=b$ の検索は，それぞれ空間変調器（データマスク）の空間シャッタの a,b に対応する部分を開閉することによって光学的に行い，両者の一致は空間/時間変化した後に電気的に検出し，加算後，レジスタに蓄える．

3, 4, 5, 7, 11, 13, 17 を法とする剰余数系で上の方式で10進6桁の数を対象とする30行30列の行列の乗算を実行する場合，通常の演算方式では 30^3 回の乗算を必要とするのに対して，LED の発光回数が565回で済む[23]．同様のアルゴリズムを純電子方式で実現した場合と比較すると，このような光・電子複合方式は，行列の次数が大きくなるほどメリットが増す[24]．

（c） そのほかの方式

Carnegie-Mellon 大の Jackson らは，**3.5**(c)で述べたものと同様な周波数多重音響光学変調器を用いた光シストリック行列ベクトル乗算器において，剰余数表現をとることによって，使用デバイスのダイナミックレンジに対する要求を減小するとともに，演算精度を向上することを試みている[25]．

また，Ohio 州立大の Habiby らは，液晶光空間変調器とホログラム表を主構成要素とする行列乗算器を提案している[26]．

4. おわりに

剰余演算の基礎に触れた後，その光学的な実現法へのいくつかの試みを紹介してきた．

これらのアプローチは千差万別であり，現状では必ずしも光剰余演算の方式として明確な方向が示されているとは思えない．むしろ，**3.** のはじめにも述べたような剰余演算と光との接点を巧妙に利用した新しい考え方が，これからも生まれてくることが期待される．そのためにも，光学的な手法と電子的な手法の系統的な比較が必要である．また，光剰余演算はそれだけで1つの独立した手法を形造るのではなく，広く情報処理一般の中の共通的な技術として位置付けられるべきであると思う．今後とも，そこで用いるデバイス（ハードウェア）とともに，光学的処理に適した剰余演算理論の進展や広い意味でのソフトウェアの研究に力を入れることが重要であろう．

終りに，本稿の内容についてご討論をいただいた電総研の大東栄夫氏及び本稿執筆にあたってお世話になった島田俊夫氏に厚くお礼申し上げる．

参考文献

1) Szabó, N. S. and Tanaka, R. I.: *Residue Arithmetic and Its Applications to Computer Technology*, 236 p., McGraw-Hill, New York (1967).
2) 高橋秀俊，石橋善弘：電子計算機による exact な計算の新方法（modulo p 演算の応用），情報処理, Vol. 1, No. 2, pp. 78-86 (1960).
3) Huang, A.: *The Implementation of a Residue Arithmetic Unit via Optical and Other Physical Phenomena, Proceeding of the* 1975 *International Optical Computing Conference*, pp. 14-18 (IEEE Cat. No. 75 CH 0941-5C, 1975).
4) 石原 聰：剰余算法を用いた光演算 (I), *O plus E*, No. 1, pp. 63-68 (1980).
5) Lehmer, D. H.: Photo-electric Number Sieve, American Mathematical Monthly, Vol. 40, pp. 401-406 (1933).
6) 石原 聰，島田潤一，桜井健二郎：光コンピュータ，電子通信学会誌, Vol. 64, No. 1, pp. 89-94 (1981).
7) Huang, A., Tsunoda, Y., Goodman, J. W. and Ishihara, S.: *Optical Computing Using Residue Arithmetic*, *Applied Optics*, Vol. 18, No. 2, pp. 149-162 (1979).
8) 石原 聰：剰余算法を用いた光演算(II), *O plus E*, No. 2, pp. 68-76 (1980).
9) Psaltis, D., Caimi, F., Casasent, D. and Goutzoulis, A.: *Decimal/Residue Conversion by Time-Integrating Correlation*, *Optics Communications*, Vol. 36, No. 3, pp. 178-180 (1981).
10) Collins Jr., S. A., Ambuel, J. and Damon, E. K.: *Numerical Optical Data Processing*, *Proceeding of the 1978 International Optical Computing Conference*, IEEE Cat. No. 78 CH 1305-2C, pp. 194-197 (1978).
11) Polky, J. N. and Miller, D. D.: *Optical Waveguide Design of an Adaptive Filter in the Residue Number System*, *Applied Optics*, Vol. 21, No. 19, pp. 3539-3551 (1982).
12) Miller, D. D. and Polky, J. N.: *A Residue*

Number System Implementation of the LMS Algorithm Using Optical Waveguide Circuits, IEEE Trans. Computers, Vol. C-32, No. 11, pp. 1013-1028 (1983).

13) Ishihara, S. and Yajima, H.: *Optical Computational Array Processors Using Optically Controlled Guided-Wave Devices, Conference Digest of the 13th Congress of the International Commission for Optics*, Science Council of Japan and Japan Society of Applied Physics, pp. 158-159 (1984).

14) Cindrich, I., Tai, A., Fienup, J. R. and Aleksoff, C. C.: *Concepts for Numerical Optical Computers, Optical Engineering*, Vol. 20, No. 4, pp. 639-650 (1981).

15) Horrigan, F. A. and Stoner, W. W.: *Residue-Based Optical Processor, Proc. SPIE*, Vol. 185, pp. 19-27 (1979).

16) Psaltis, D. and Casasent, D.: *Optical Residue Arithmetic: a Correlation Approach, Applied Optics*, Vol. 18, No. 2, pp. 163-171 (1979).

17) Guest, C. C. and Gaylord, T. K.: *Truth-Table Look-Up Optical Processing Utilizing Binary and Residue Arithmetic, Applied Optics*, Vol. 19, No. 7, pp. 1201-1207 (1980).

18) Guest, C. C., Mirsalehi, M. M. and Gaylord, T. K.: *Residue Number System Truth-Table Look-Up Processing——Moduli Selection and Logical Minimization, IEEE Trans. Computers*, Vol. C-33, No. 10, pp. 927-931 (1984).

19) Gaylord, T. K., Mirsalehi, M. M. and Guest, C. C.: *Optical Digital Truth Table Look-Up Processing, Optical Engineering*, Vol. 24, No. 1, pp. 48-58 (1985).

20) Mirsalehi, M. M. and Gaylord, T. K.: *Multi-Level Coded Residue-Based Content-Addressable-Memory Optical Computing, Technical Digest of Topical Meeting on Optical Computing*, Optical Society of America, WB1 (1985).

21) 安東 滋, 関根征士, 関川和成：多重エンボストホログラム(II)光学的剰余演算研究への応用, 第44回応用物理学会学術講演会講演予稿集, pp. 72 (1983).

22) 関川和成, 安東 滋, 関根征士：剰余算法によるマトリックス乗算用光ディジタル計算機（I）. 昭和59年度電子通信学会総合全国大会予稿集, 4-84 (1984).

23) 安東 滋, 関川和成, 関根征士：同上（II）, 昭和59年度電子通信学会総合全国大会予稿集, 4-85 (1984).

24) 同上：マトリックス乗算と光コンピュータ, 昭和59年度文部省科学研究費補助金総合研究（A）「光コンピュータの基礎に関する総合的研究」第1回・第2回研究会論文集 pp. 9-12 (1984).

25) Jackson, J. and Casasent, D.: *Optical Systolic Array Processor Using Residue Arithmetic, Applied Optics*, Vol. 22, No. 18, pp. 2817-2821 (1983).

26) Habiby, S. F. and Collins Jr., S. A.: *Design of an Optical Residue Arithmetic Matrix Vector Multiplier Using Holographic Table Lookup, Technical Digest of Topical Meeting on Optical Computing* Optical Society of America, TuD 4 (1985).

（昭和60年7月8日受付）