中国剰余定理の高速演算と数値実験

Fuse, Mitsuo / Nagasaka, Kenji / 長坂, 建二 / 布施, 光男

(出版者 / Publisher)
法政大学工学部
(雑誌名 / Journal or Publication Title)
法政大学工学部研究集報 / 法政大学工学部研究集報
(巻 / Volume)
29
(開始ページ / Start Page)
97
(終了ページ / End Page)
113
(発行年 / Year)
1993-03
(URL)
https://doi.org/10.15002/00003859

中国剰余定理の高速演算と数値実験

布施光男・長坂建二

Fast algorithm and numerical experiments of the Chinese Remainder Theorem

Mitsuo FUSE and Kenji NAGASAKA

Abstract

A fast algorithm of the Chinese Remainder Theorem is proposed recently by K. Nagasaka, C.－W. Ho and J.－S. Shiue. We have studied numerically two algorithms of the Chinese Remainder Theorem for the ring of integers and polynomial rings over finite fields by using computer algebra system. This paper shows that our fast algorithm is better than the ordinary algorithm in processing times.

0．はじめに

中国剰余定理は昔から中国で知られていて，孫子の『孫子算経』に示されているという．この書物の年代は西暦400年ころといわれているが，明らかではない．これをニーダム（Joseph Needham）の『中国の科学と文明』第4巻数学編より引用すると表1の通りである．これを現代風に書くと次のような連立合同式で表せる．

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

ところで，中国剰余定理は今日においても，大きな整数を扱う計算アルゴリスムとして重要である．それは大きな数 x の計算を直接行うのではなく，互いに素である法 m_1，m_2，……，m_k を用意し，その数の剰余 $x \pmod{m_1}$，$x \pmod{m_2}$，……，$x \pmod{m_k}$ を用いて，間接的に計算を行う算法である．中国剰余定理は大きな数を扱うので，高速のアルゴリスム

＊本研究は，文部省科学研究費一般研究（C）「計算アルゴリスムの開発と基礎理論」研究代表者：長坂建二，課題番号：03640233の援助を受けた．

が求められる．近年，中国剰余定理についての新しい高速計算法が，長坂－Ho－Shiue「1」によって提案された．

本稿はこの新しいアルゴリスムと，従来から知られている通常の計算法について，次のような観点から，二つの数式処理言語上で計算システムを開発し，計算時間の検討を行った．

①中国剰余定理の数式処理言語上での新旧アルゴリスムの記述．

②整数環における高速計算法と通常の計算法による計算時間の比較・検討．

③中国剰余定理の高速計算法の有限体上の多項式環への拡張と，通常の計算法による計算時間との比較・検討．

これらについて一定の成果が得られたので報告する．

今有物不知其数
三三数之賸二
五五数之賸三
七七数之賸二
問物幾何
（『孫子算經』下巻、十葉裏）

表1．『孫子算経』の原文

1．中国剰余定理

〔中国剰余定理〕

m_1，m_2，……，m_k が，互いに素である自然数とする．このとき，k 個の連立合同式

$$(1.\ 1)\qquad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

を同時に満たす解 x は，mod M で唯一つ存在する．ここで，$M=m_1m_2\cdots\cdots m_k$ である．これを中国剰余定理という．

〔証明〕

（1．1）が mod M で唯一つの解をもつことを証明しよう．いま，（1．1）の解を x，x_0 とすると，

$$(1.\ 2)\qquad \begin{cases} x \equiv a_i \pmod{m_i} \\ x_0 \equiv a_i \pmod{m_i} \end{cases} \qquad i=1,\ 2,\ \cdots\cdots,\ k$$

がすべての i について成り立つ．それぞれの i について二式の差をとれば，

$$x - x_0 \equiv 0 \pmod{m_i}, \qquad i=1,\ 2,\ \cdots\cdots,\ k$$

となる．したがって，$x-x_0$ はすべての i に対して m_i の倍数であり，どの m_i，m_j（$i \neq j$）も互いに素であるから，$x-x_0$ は $M=m_1m_2\cdots\cdots m_k$ で割り切れる．すなわち，

$$(1.\ 3)\qquad x \equiv x_0 \pmod{M}$$

であり，（1．1）の解は mod M で唯一つに定まる．

証明を完成するには，解が少なくとも一つ存在することを証明しなければならない．

＜方法1＞

y_i が $0 \leqq y_i \leqq m_i - 1$，$i = 1, 2, \cdots\cdots, k$ を満たして独立に動くとき，k 次元整数ベクトル $(y_1, y_2, \cdots\cdots, y_k)$ は，ちょうど M 個ある．また，x が M 個の異なる値 $0 \leqq x \leqq M-1$ を動くならば，k 次元のベクトル $(x \bmod m_1, x \bmod m_2 \cdots\cdots, x \bmod m_k)$ は M 個の異なる値を動く．以上より $(y_1, y_2, \cdots\cdots, y_k) = (a_1, a_2, \cdots\cdots, a_k)$ として

$$(1.4) \qquad (x \bmod m_1, x \bmod m_2, \cdots\cdots, x \bmod m_k) = (a_1, a_2, \cdots\cdots, a_k)$$

となる x が mod M で存在する．

＜方法2＞

いま，M_i を次のように定義しよう．

$$M_i = M / m_i = m_1 m_2 \cdots\cdots m_{i-1} m_{i+1} \cdots\cdots m_k, \quad i = 1, 2, \cdots\cdots, k$$

すると，$(M_i, m_i) = 1$ である．

次に，$\phi(\cdot)$ をオイラーの関数として

$$(1.5) \qquad y_i = M^{\phi(m_i)} \qquad i = 1, 2, \cdots\cdots, k$$

とおく．$(M_i, m_i) = 1$ であるから，フェルマーの小定理によって，

$$y_i \equiv 1 \pmod{m_i}, \quad i = 1, 2 \cdots\cdots, k$$

が得られる．

M_i の定義より，$y_i \equiv 0 \pmod{m_j}$，$(i \neq j)$ であるから，

$$x = a_1 y_1 + a_2 y_2 + \cdots\cdots + a_k y_k$$

は（1．1）の一つの解である．

〔証明終〕

〔注意〕

（1．5）の y_i とおくかわりに，次の，

$$(1.6) \qquad M_i z_i \equiv 1 \pmod{m_i}, \quad i = 1, 2, \cdots\cdots, k$$

を満たす z_i をそれぞれの i についてとると，

$$(1.7) \qquad x = a_1 M_1 z_1 + a_2 M_2 z_2 + \cdots\cdots + a_k M_k z_k$$

は（1．1）の解である．また，（1．6）の解を得ることは次の不定方程式を解くことと同値である．

$$(1.8) \qquad M_i z_i - m_i y_i = 1.$$

2．中国剰余定理の高速計算法

この節は，長坂－Ho－Shiue が提案した計算法について述べ，その証明も与える．

〔定理1〕

中国剰余定理と同じ仮定のもとで，（1．1）は次式と同値である．

$$(2.\ 1)\qquad \left(\sum_{i=1}^{k} b_i M_i\right) x \equiv \sum_{i=1}^{k} a_i b_i M_i \pmod{M}$$

ここで，b_i は $(b_i,\ m_i) = 1$　$i = 1,\ 2,\ \cdots\cdots,\ k$ であるような任意の整数，

$M = m_1 m_2 \cdots\cdots m_k$,

$M_i = M / m_i$,　$i = 1,\ 2,\ \cdots\cdots,\ k$

である．

〔補題1〕

定理1と同じ条件のもとで，（1．1）は次の連立合同式（2．2）と同値である．

$$(2.\ 2)\qquad \begin{cases} M_1 x \equiv a_1 M_1 \pmod{M} \\ M_2 x \equiv a_2 M_2 \pmod{M} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ M_{k-1} x \equiv a_{k-1} M_{k-1} \pmod{M} \\ \left(\sum_{i=1}^{k} b_i M_i\right) x \equiv \sum_{i=1}^{k} a_i b_i M_i \pmod{M} \end{cases}$$

〔補題1の証明〕

（1．1）の一つの解を x とすれば，

$$x - a_i = c_i m_i,\qquad i = 1,\ 2,\ \cdots\cdots,\ k$$

が成り立つ．ここで，c_i は整数である．いま，上式の両辺に M_i を掛けると，すべての i に対して次式が成り立つ．

$$M_i x - M_i a_i = c_i m_i M_i = c_i M,\qquad i = 1,\ 2,\ \cdots\cdots,\ k$$

これを合同式で書くと，

$$(2.\ 3)\qquad \begin{cases} M_1 x \equiv M_1 a_1 \pmod{M} \\ M_2 x \equiv M_2 a_2 \pmod{M} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ M_{k-1} x \equiv M_{k-1} a_{k-1} \pmod{M} \\ M_k x \equiv M_k a_k \pmod{M} \end{cases}$$

となる．（2．2）の $k-1$ 番目までの式は，（2．3）の $k-1$ 番目までの式と同じである．（2．3）の各合同式の両辺に b_i をかけて加えれば（2．2）の k 番目の式が得られる．これで，（2．3）から（2．2）が導びかれた．

次に，（2．2）から（1．1）を導びく．

$$M_i x \equiv a_i M_i \pmod{M}\qquad i = 1,\ 2,\ \cdots\cdots,\ k-1$$

が成り立つ．$(M_i,\ m_i) = 1$ より，合同式の両辺を M_i で割って

$$x \equiv a_i \pmod{m_i} \qquad i = 1, 2, \cdots\cdots, k-1$$

が導びかれる．次に，（2．2）の最後の合同式から

$$b_i M_i x \equiv b_i a_i M_i \pmod{M} \qquad i = 1, 2, \cdots\cdots, k-1$$

を引いて

$$b_k M_k x \equiv b_k a_k M_k \pmod{M}$$

を得る．ここで，両辺をM_kで割って，$(M_k, m_k) = 1$より

$$b_k x \equiv b_k a_k \pmod{m_k}$$

が成立する．ここで，$(b_k, m_k) = 1$の仮定より

$$x \equiv a_k \pmod{m_k}$$

が導びかれる．

以上より，（2．2）から（1．1）が導びかれた．

〔補題1の証明終〕

〔補題2〕

定理1と同じ条件のもとで，Mと$\sum_{i=1}^{k} b_i M_i$は互いに素である．

〔補題2の証明〕

Mと$\sum_{i=1}^{k} b_i M_i$の最大公約数をgとする．$(m_i, m_j) = 1$（$i \neq j$）であるから，gが$M = \prod_{i=1}^{k} m_i$を割り切るということは，gはあるm_iを割り切り，他のm_j（$i \neq j$）を割り切らない．ここで，m_iは$M_j = M/m_j$（$i \neq j$）の因数であるから，gはM_j（$i \neq j$）を割り切る．したがって，gは$\sum_{j \neq i} b_j M_j$を割り切る．gは$\sum_{i=1}^{k} b_i M_i$を割り切るから，gは

$$\sum_{i=1}^{k} b_i M_i - \sum_{j \neq i} b_j M_j = b_i M_i$$

を割り切る．gはm_iを割り切ると仮定して，$(b_i, m_i) = 1$よりgはb_iを割り切ることはない．したがって，gが$M_i = M/m_i$を割り切ることになるが，これはgがm_j（$i \neq j$）を割り切らないことから，$g = 1$とならねばならない．つまり，Mと$\sum_{i=1}^{k} b_i M_i$は互いに素である．

〔補題2の証明終〕

〔定理1の証明〕

補題1により，中国剰余定理の連立合同式（1．1）は，（2．2）と同値であることがわかった．ここで，（2．2）のk番目の合同式

$$\left(\sum_{i=1}^{k} b_i M_i\right) x \equiv \sum_{i=1}^{k} a_i b_i M_i \pmod{M}$$

に着目する．補題2より，$\sum_{i=1}^{k} b_i M_i$はMと互いに素である．したがって，この合同式の解x_0は，mod Mで唯一つに定まる．一方，連立合同式（1．1）の解はmod Mで唯一つ存在する．ということは，合同式（2．1）の解は，連立合同式（2．2）の解であり，これは補題1より，中国剰余定理の連立合同式（1．1）の解である．

〔定理1の証明終〕

3．整数環での中国剰余定理の計算アルゴリスム

中国剰余定理を解くには，通常の方法によれば（1．6）のk個の合同式を，高速計算法によれば（2．1）の一つの合同式を解けばよいことがわかった．ここで，1元1次合同式の解法を復習しておく．

3.1　1元1次合同式の解法

fとgが互いに素と仮定して，1元1次合同式は（3．1）で表せる．

（3．1）　　$f \cdot x \equiv a \pmod{g}$

いま，（3．1）の解法を考える．

一般に，fとgの最大公約数は，以下のようにユークリッドの互除法を用いて求められることが知られている．まず，$r_0=f$，$r_1=g$とおき，f/gの商をq_1，剰余をr_2とする．以下割り算を繰り返して，互除法は次のように書ける．

（3．2）
$$\begin{cases} r_0=q_1r_1+r_2, & 0\leqq r_2<r_1, \\ r_1=q_2r_2+r_3, & 0\leqq r_3<r_2, \\ \cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots \\ r_{s-2}=q_{s-1}r_{s-1}+r_s, & 0\leqq r_s<r_{s-1}, \\ r_{s-1}=q_sr_s+r_{s+1}, & r_{s+1}=0, \end{cases}$$

求めたr_sが，fとgの最大公約数$(f,\ g)=r_s$である．

次に〔2〕にしたがって，

（3．3）　　$r_s=u_sf+v_sg$

を満たす$(u_s,\ v_s)$の構成法を示す．

$$\begin{cases} u_0=1,\ v_0=0, \\ u_1=0,\ v_1=1, \end{cases}$$

とおく．すると，$r_0=f$，$r_1=g$とおいたから，$j=0$，1に対して

$$r_j=u_jf+v_jg$$

が成り立つ．$j=2$，3，……，sについて，数列$\{u_j\}$，$\{v_j\}$を，次の漸化式

（3．4）
$$\begin{cases} u_j=u_{j-2}-q_{j-1}u_{j-1} & j=2,\ 3,\ \cdots\cdots,\ s \\ v_j=v_{j-2}-q_{j-1}v_{j-1} & j=2,\ 3,\ \cdots\cdots,\ s \end{cases}$$

で定める．（3．2）の最初の式は

$$\begin{aligned} r_2&=r_0-q_1r_1 \\ &=f-q_1g \end{aligned}$$

と変形される．ここで，（3．4）より，$u_2=1$，$v_2=-q_1$であるから，上式に代入すると

$$r_2=u_2f+v_2g$$

が成り立つ．同様に$u_3=-q_2$，$v_3=1+q_1q_2$より

$$r_3 = r_1 - q_2 r_2$$
$$= g - q_2 (f - q_1 g)$$
$$= -q_2 f + (1 + q_1 q_2) g$$
$$= u_3 f + v_3 g$$

となる．$j = i - 1$（$i \geqq 4$）まで

$$r_j = u_j f + v_j g$$

が成り立つと仮定すると（数学的帰納法の仮定）

$$r_i = r_{i-2} - q_{i-1} r_{i-1}$$
$$= (u_{i-2} f + v_{i-2} g) - q_{i-1} (u_{i-1} f + v_{i-1} g)$$
$$= (u_{i-2} - q_{i-1} u_{i-1}) f + (v_{i-2} - q_{i-1} v_{i-1}) g$$
$$= u_i f + v_i g$$

が，（3．4）より成り立つ．したがって，（3．3）を満たす（u_n，v_n）は，（3．4）により帰納的に構成された．

f と g が互いに素と仮定したから，$r_n = 1$，したがって（3．3）は

$$1 = u_n f + v_n g$$

となる．これから，合同式

（3．5）　$$f u_n \equiv 1 \pmod{g}$$

が導びかれる．両辺に a をかけて，（3．1）の1元1次合同式の解を

（3．6）　$$x \equiv u_n a \pmod{g}$$

として求めることができる．

3．2　中国剰余定理の計算アルゴリズム

（1．1）の中国剰余定理の通常の解法による解は，（1．6）から k 個の逆元 z_i を求めて，（1．7）を用いる．M_i と m_i の最大公約数は1であるから，（3．4）により u_i，すなわち M_i の逆元を求めればよい．合同式が k 個あるので，これを k 回繰り返すことによって，k 個の逆元が求まる．

次に高速計算法のアルゴリズムであるが，これは合同式（2．1）を解くから，（3．4）を用いて一つの逆元を求めればよい．上述したように，通常の計算法では k 個の合同式を解く必要があるが，長坂－Ho－Shiue の結果によれば唯一の合同式を解けばよいことがわかる．

Lamé の定理（〔2〕参照）より，理論的な計算回数は後者の計算法の方が（最悪の場合でも）少なくてすむことがわかっている（〔1〕）．ただ，整数環の場合に高速計算法では，（2．1）からわかるように，大きな整数の計算をするため，数式処理言語が必要になる．実際の演算を行った場合どの程度の改善が見られるかということが，本研究の最初の課題である．（第5節参照）

4．有限体上の多項式環への拡張と計算法

4.1　有限体上の多項式環への拡張

元の数を q（$q=p^n$，p：素数）とする有限体を $F_q=GF(q)$ とし，F_q 上の多項式環を，x を不定元として $F_q[x]$ と書く．このとき，中国剰余定理の（1．1）は（4．1）に書き換えられる．

$$(4.1)\qquad \begin{cases} y(x)\equiv a_1(x) \pmod{m_1(x)} \\ y(x)\equiv a_2(x) \pmod{m_2(x)} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ y(x)\equiv a_k(x) \pmod{m_k(x)} \end{cases}$$

ただし，$(m_i(x),\ m_j(x))=1,\ i\neq j$．

ここで，

$$m_1(x),\ m_2(x),\ \cdots\cdots,\ m_k(x)\in F_q[x],$$
$$a_1(x),\ a_2(x),\ \cdots\cdots,\ a_k(x)\in F_q[x],$$

である．ユークリッドの互除法が $F_q[x]$ においても適用できるから（4．1）を満たす解 $y(x)$ は mod $M(x)$ で唯一つ存在する．それを $a_0(x)$ と書くと

$$(4.2)\qquad y(x)\equiv a_0(x) \pmod{M(x)}$$

ただし，$M(x)=\prod_{i=1}^{k} m_i(x)$，$\quad a_0\in F_q[x]$，

となる．これが，整数環から有限体上の多項式環への拡張である．したがって，通常の解法による（4．2）の計算法は，整数環の場合と同様である．いま，$z_i(x)\in F_q[x]$ として，多項式環における逆元 $z_i(x)$ を求める．つまり

$$(4.3)\qquad M_i(x)\cdot z_i(x)\equiv 1 \pmod{m_i(x)}$$
$$i=1,\ 2,\ \cdots\cdots,\ k$$

ただし，$M_i(x)=M(x)/m_i(x)$ とした．

多項式環における中国剰余定理の求める解は

$$(4.4)\qquad y(x)=\sum_{i=1}^{k} a_i(x)\ M_i(x)\ z_i(x)$$
$$\equiv a_0(x) \pmod{M(x)}$$

である．

同様にして，長坂－Ho－Shiue の高速計算法についても，（2．1）に対応する合同式は（4．5）である．

$$(4.5)\qquad \left(\sum_{i=1}^{k} b_i(x)M_i(x)\right)\ f(x)$$
$$\equiv \sum_{i=1}^{k} a_i(x)\,b_i(x)M_i(x) \pmod{M(x)}$$

ただし，$b_i(x)\in F_q[x]$，$(b_i(x),\ m_i(x))=1$ である．

4.2　多項式環における計算法

有限体上の多項式環における演算は整数環での演算と同様にできる．いま，多項式環の元（多項式）を $f(x)$，$g(x)\in F_q[x]$ とおいて合同式

$$f(x)\cdot y(x)\equiv a_0(x) \pmod{g(x)} \qquad (4.6)$$

を解くことを考えよう．$f(x)$ と $g(x)$ の最大公約多項式を $(f(x),\ g(x)) = r_s(x)$ と書く．

$r_s(x)$は多項式環上のユークリッドの互除法によって求まる．つまり，$r_0(x) = f(x)$，$r_1(x) = g(x)$ とおいて，$f(x)/g(x)$ の商を $q_1(x)$ とし，剰余を $r_2(x)$ とすれば，（3．3）に対応して（4．7）で表せる．

$$(4.7)\quad \begin{cases} r_0(x) = q_1(x)r_1(x)+r_2(x), \\ \qquad\qquad 0\leqq \deg(r_2(x)) < \deg(r_1(x)), \\ r_1(x) = q_2(x)r_2(x)+r_3(x), \\ \qquad\qquad 0\leqq \deg(r_3(x)) < \deg(r_2(x)), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ r_{s-2}(x) = q_{s-1}(x)r_{s-1}(x)+r_s(x), \\ \qquad\qquad 0\leqq \deg(r_s(x)) < \deg(r_{s-1}(x)), \\ r_{s-1}(x) = q_s(x)r_s(x)+r_{s+1}(x),\ \deg(r_{s+1}(x)) = 0, \end{cases}$$

$\deg(r_j(x))$ は，$r_j(x)$ の次数である．ここで，$r_{s+1}(x)\in F_q$ であるから，$q_s(x)$，$r_s(x)$ の定数を調整して，$r_{s+1}(x)=0$ とできる．その結果，$r_s(x)$ は（4．7）より求まり，

$$(f(x),\ g(x)) = c\, r_s(x) \qquad (4.8)$$

となる．ここで，$c\in F_q$ である．整数環における剰余の不等式 $0\leqq r_{j+1}<r_j$ が，多項式の次数の不等式 $0\leqq\deg(r_{j+1}(x)) <\deg(r_j(x))$ に変ったことに注意せよ．

次に

$$r_j(x)=u_j(x)f(x)+v_j(x)g(x) \quad j=0,\ 1,\ \cdots\cdots,\ s \qquad (4.9)$$

をみたす $F_q[x]$ の多項式列 $\{u_s(x)\}$，$\{v_s(x)\}$ を構成する．

まず，

$$\begin{cases} u_0(x)=1,\ v_0(x)=0 \\ u_1(x)=0,\ v_1(x)=1 \end{cases}$$

とおき，$j\geqq 2$ に対しては

$$\begin{cases} u_j(x)=u_{j-2}(x)-q_{j-1}(x)u_{j-1}(x) \\ v_j(x)=v_{j-2}(x)-q_{j-1}(x)v_{j-1}(x) \end{cases} \qquad (4.10)$$

$$j=2,\ 3,\ \cdots\cdots,\ s$$

とおけばよい．$f(x)$ と $g(x)$ が互いに素であるならば，$r_s(x)=1$ であるから（4．9）は

$$1=u_s(x)f(x)+v_s(x)g(x)$$

となる．したがって

$$f(x)\cdot u_1(x)\equiv 1 \pmod{g(x)}$$

となる．つまり，$u_1(x)$は，mod $g(x)$についての$f(x)$の逆元である．したがって，合同式（4．6）の解$y(x)$は

$$y(x)\equiv u_1(x)a_0(x) \pmod{g(x)} \qquad (4.11)$$

として求めることができる．補題2と同様に，$F_q[x]$においても$\sum_{i=1}^{k} b_i(x)M_i(x)$と$M(x)$は互いに素であるから，（4．5）の解を今述べたアルゴリスムにより求めることができる．

4.3　多項式環における計算アルゴリスム

（4．1）で表された有限体上の多項式環の中国剰余定理の解を求める計算アルゴリスムは，第3節3．2で述べた整数環の場合と同様に考えられる．

通常の解法による解は，（4．3）から逆元$z_i(x)$をk個求めることによって，（4．4）が解となる．また，高速計算法の場合には，合同式（4．5）を（4．6）の解法にならって解けばよい．

5．中国剰余定理の数式処理言語を用いるアルゴリスムと計算数値例

5．1　通常の計算法

(1) 計算アルゴリスム

第3節の3．2で述べた計算アルゴリスムから次のフローチャートが導びかれる．

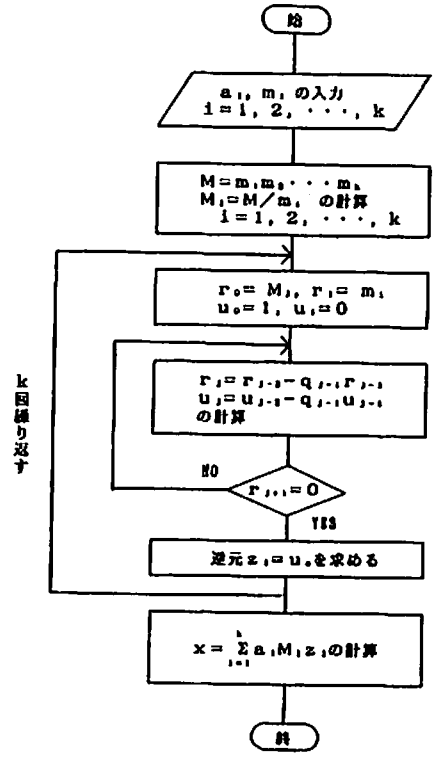

図1．　通常計算法のフローチャート

(2) 整数環上の中国剰余定理の計算

使用した計算機と言語は次の通りである.

1．使用計算機　PC－9801　RA（NEC）

2．言語　UBASIC, Ver．4．3，作成者　木田　祐司

プログラムを示すと次の通りである.

```
 10 ' ***** ORDINARY  METHOD *****
 20 input "n=";N
 30 dim A(N),M(N),MM(N),Q(10),R(10),S(10),Y(10)
 40 for I=1 to N
 50     input "a=";A(I)
 60     input "法 m=";M(I)
 70 next I
 80 print time
 90 for LL=1 to 1000
100 IM=1
110 for II=1 to N
120     IM=IM*M(II)
130 next II
140 for J=1 to N
150     MM(J)=IM¥M(J)
160 next J
170 S(0)=1:S(1)=0
180 for I=1 to N
190     L1=MM(I):J1=M(I)
200     K=0
210   *hajime
220     K=K+1:Q(K)=L1¥J1
230     R(K)=L1@J1:M1=R(K)
240     if M1=0 goto *saki
250     L1=J1:J1=M1
260     goto *hajime
270   *saki
280       for J=2 to K
290          S(J)=S(J-2)-S(J-1)*Q(J-1)
300       next J
310     if S(K)>0 goto 340
320     Y(I)=M(I)+S(K)
330     goto *owari
340     Y(I)=S(K)
350   *owari
360 next I
370 U=0
380 for I=1 to N
390     U=U+A(I)*MM(I)*Y(I)
400 next I
410 if U>IM goto 440
420 X=U
430 goto 450
440 X=U@IM
450 next LL
460 print time
470 print "***  連立合同式の解  ***"
480 print "x=",X," ( mod ",IM,")"
490 end
```

図2.　整数環上のＵＢＡＳＩＣプログラム（通常計算法）

＜計算例1＞

$$\begin{cases} x \equiv 23 \pmod{61} \\ x \equiv 83 \pmod{229} \\ x \equiv 167 \pmod{503} \\ x \equiv 271 \pmod{647} \\ x \equiv 701 \pmod{977} \end{cases}$$

＊＊＊　連立合同式の解　＊＊＊

$$x \equiv 167164470963 6 \pmod{444152536643 3}$$

このときの計算に要した時間は，34(ms)である．

＜計算例2＞

$$\begin{cases} x \equiv 2 \pmod{31} \\ x \equiv 3 \pmod{37} \\ x \equiv 5 \pmod{41} \\ x \equiv 7 \pmod{43} \\ x \equiv 11 \pmod{47} \\ x \equiv 13 \pmod{53} \\ x \equiv 17 \pmod{61} \\ x \equiv 19 \pmod{67} \\ x \equiv 23 \pmod{71} \\ x \equiv 29 \pmod{73} \end{cases}$$

＊＊＊　連立合同式の解　＊＊＊

$$x \equiv 422923534342242 49 \pmod{106702674290291971}$$

この計算に要した時間は165(ms)である．

(3) 有限体上の多項式環上の中国剰余定理の計算

1．使用計算機　M780／10　(FACOM)

2．言語　REDUCE 3．3　(The RAND Corporation)

プログラムを示すと次のようになる．

```
PROCEDURE  AMARIBIG(X,Y);  %*** X>Y ***
  BEGIN
        SCALAR   X,Y,C,R;
        SETMOD   7$
        ON MODULAR$
        R:=REMAINDER(X,Y);C:=1;
  L1:   IF R=0 THEN RETURN C;
        X:=Y;Y:=R;
        R:=REMAINDER(X,Y);
        C:=C+1;GO TO L1;
  END;
PROCEDURE  AMARI(X,Y);  % *** X<Y ***
  BEGIN
        SCALAR   X,Y,C,R;
        SETMOD   7$
        ON MODULAR$
        R:=REMAINDER(Y,X);C:=1;
  L1:   IF R=0 THEN RETURN C;
        Y:=X;X:=R;
        R:=REMAINDER(Y,X);
        C:=C+1;GO TO L1;
  END;
PROCEDURE  SHOBIG(X,Y,C);  % *** X>Y ***
  BEGIN
        SCALAR   X,Y,C,R,Q,TT,TT1,TT2;
        ON MODULAR$
        SETMOD   7$
        TT1:=1;TT2:=0;
  L2:   IF C=0 THEN RETURN TT;
        R:=REMAINDER(X,Y);Q:=(X-R)/Y;
        TT:=TT1-TT2*Q;TT1:=TT2;TT2:=TT;
        X:=Y;Y:=R;C:=C-1;GO TO L2;
  END;
PROCEDURE  SHO(X,Y,C);  % *** X<Y ***
  BEGIN
        SCALAR   X,Y,C,R,Q,TT,TT1,TT2;
        ON MODULAR$
        SETMOD   7$
        TT1:=0;TT2:=1;
  L2:   IF C=0 THEN RETURN TT;
        R:=REMAINDER(X,Y);Q:=(Y-R)/X;
        TT:=TT1-TT2*Q;TT1:=TT2;TT2:=TT;
        Y:=X;X:=R;C:=C-1;GO TO L2;
  END;
% ***   ORDINARY  METHOD  ***
ON TIME$
SETMOD 7$
ON MODULAR$
A1:=2$
A2:=3*X+2$
A3:=5*X**2+6*X+6$
M1:=X+3$
M2:=X**2+4*X+4$
M3:=X**3+2*X+6$
M:=M1*M2*M3;
MM1:=M/M1$
MM2:=M/M2$
MM3:=M/M3$
C1:=AMARIBIG(MM1,M1)$
C2:=AMARIBIG(MM2,M2)$
C3:=AMARI(MM3,M3)$
D1:=SHOBIG(MM1,M1,C1-1)$
D2:=SHOBIG(MM2,M2,C2-1)$
D3:=SHO(MM3,M3,C3-1)$
Y:=A1*MM1*D1+A2*MM2*D2+A3*MM3*D3;
END;
```

図3.　多項式環上のＲＥＤＵＣＥプログラム（通常計算法）

＜計算例3＞

$$\begin{cases} y(x) \equiv 2 \pmod{x+3} \\ y(x) \equiv 3x+2 \pmod{x^2+4x+4} \\ y(x) \equiv 5x^2+6x+6 \pmod{x^3+2x+6} \end{cases}$$

ここで，$F_7=\{0, 1, 2, 3, 4, 5, 6\}$

$F_7[x] \ni a_n x^n + a_{n-1} x^{n-1} + \cdots\cdots + a_1 x + a_0$

$a_i \in F_7$

$$y(x) \equiv 4(x^5+3x^4+3x^3+x^2+4x+4) \pmod{x^6+4x^4+4x^3+4x^2+x+2}$$

この計算時間は48(ms)である．

5．2　高速計算法のフローチャートと計算例

(1)　フローチャート

計算式の（2．1）と第4節の4．3で述べた計算アルゴリズムから次のフローチャートが得られる．

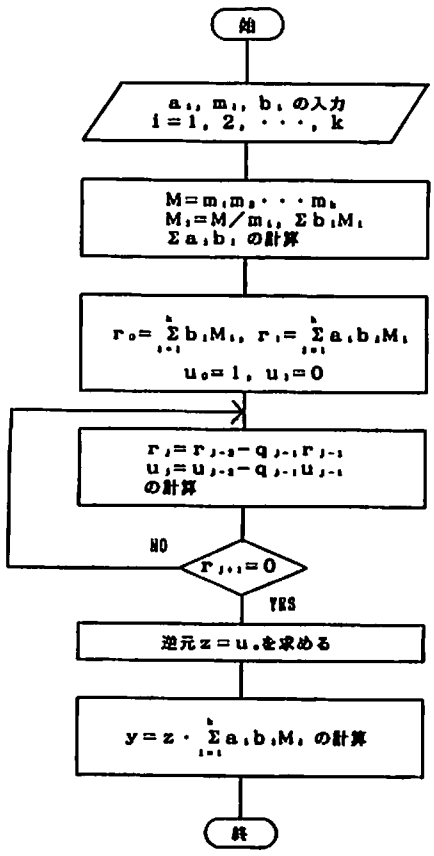

図4.　高速計算法のフローチャート

(2) 整数環上の中国剰余定理の計算

＜計算例４＞

計算例１の問題を高速計算法によって計算させた結果，２２(ms)の計算時間を要した．通常の計算法に要した時間が３４(ms)であるから，約３３％の短縮ができたことになる．

＜計算例５＞

計算例２の問題を高速計算法を使って計算した．計算に要した時間は１３４（ms）であった．したがって，約２０％短縮されたことになる．

プログラムを示すと次のようになる．

```
10 ' *****  FAST METHOD  *****
20 input "n=";N
30 dim A(N),M(N),MM(N),B(N),T(18),Q(18),R(18),V(18)
40 for I=1 to N
50     input "a= ";A(I)
60     input "法 p=";M(I)
70     input "b= ";B(I)
80 next I
90 print time
100 for JJ=1 to 1000
110 IM=1
120 for II=1 to N
130     IM=IM*M(II)
140 next II
150 for J=1 to N
160     MM(J)=IM\M(J)
170 next J
180 BM=0:U=0
190 for IZ=1 to N
200     CM=B(IZ)*MM(IZ)
210     BM=BM+CM
220 next IZ
230 for I=1 to N
240     DM=A(I)*B(I)*MM(I)
250     U=U+DM
260 next I
270 if BM>0 goto 290
280 BM=-BM:U=-U
290 if U>0 goto 330
300 if abs(U)<IM goto 320
310 C=abs(U)@IM:U=IM-C:goto 330
320 U=IM+U
330 if BM>IM goto 420
340 T(0)=0:T(1)=1
350 L1=IM:J1=BM
360 K=0
370 K=K+1:Q(K)=L1\J1
380 R(K)=L1@J1:M1=R(K)
390 if M1=0 goto *saki
400 L1=J1:J1=M1
410 goto 370
420 V(0)=1:V(1)=0
430 L1=BM:J1=IM:K=0
440 K=K+1:Q(K)=L1\J1
450 R(K)=L1@J1
460 if R(K)=0 goto *muko
470 L1=J1:J1=R(K)
480 goto 440
490 *saki
500 for I=2 to K
510     T(I)=T(I-2)-T(I-1)*Q(I-1)
520 next I
530 S=T(K):goto 590
540 *muko
550 for I=2 to K
560     V(I)=V(I-2)-V(I-1)*Q(I-1)
570 next I
580 S=V(K)
590 if S>0 goto 630
600 D=IM+S:SS=D*U
610 if SS<IM goto 670
620 goto 650
630 SS=S*U
640 if SS<IM goto 670
650 X=SS@IM
660 goto *owari
670 X=SS
680 *owari
690 next JJ
700 print time
710 print "***  連立合同式の解  ***"
720 print "x=",X," ( mod ",IM,")"
730 end
```

図5.　整数環上のＵＢＡＳＩＣプログラム（高速計算法）

(3) 有限体上の多項式環上の中国剰余定理の計算

＜計算例6＞

計算例3の問題を高速計算法によって計算した．その結果，計算に要した時間は37(ms)であった．通常の計算法では48(ms)なので，約23%の短縮ができたことになる．

プログラムを次に示しておく．

```
PROCEDURE  AMARIBIG(X,Y);  %*** X>Y ***
  BEGIN
        SCALAR   X,Y,C,R;
        SETMOD   7$
        ON MODULAR$
        R:=REMAINDER(X,Y);C:=1;
  L1:   IF R=0 THEN RETURN C;
        X:=Y;Y:=R;
        R:=REMAINDER(X,Y);
        C:=C+1;GO TO L1;
  END;
PROCEDURE  AMARI(X,Y);  % *** X<Y ***
  BEGIN
        SCALAR   X,Y,C,R;
        SETMOD   7$
        ON MODULAR$
        R:=REMAINDER(Y,X);C:=1;
  L1:   IF R=0 THEN RETURN C;
        Y:=X;X:=R;
        R:=REMAINDER(Y,X);
        C:=C+1;GO TO L1;
  END;
PROCEDURE  SHOBIG(X,Y,C);  % *** X>Y ***
  BEGIN
        SCALAR   X,Y,C,R,Q,TT,TT1,TT2;
        ON MODULAR$
        SETMOD   7$
        TT1:=1;TT2:=0;
  L2:   IF C=0 THEN RETURN TT;
        R:=REMAINDER(X,Y);Q:=(X-R)/Y;
        TT:=TT1-TT2*Q;TT1:=TT2;TT2:=TT;
        X:=Y;Y:=R;C:=C-1;GO TO L2;
  END;
PROCEDURE  SHO(X,Y,C);  % *** X<Y ***
  BEGIN
        SCALAR   X,Y,C,R,Q,TT,TT1,TT2;
        ON MODULAR$
        SETMOD   7$
        TT1:=0;TT2:=1;
  L2:   IF C=0 THEN RETURN TT;
        R:=REMAINDER(X,Y);Q:=(Y-R)/X;
        TT:=TT1-TT2*Q;TT1:=TT2;TT2:=TT;
        Y:=X;X:=R;C:=C-1;GO TO L2;
  END;
% ***   FAST  METHOD  ***
ON TIME$
SETMOD 7$
ON MODULAR$
A1:=2$
A2:=3*X+2$
A3:=6*X**2+6*X+6$
B1:=1$
B2:=1$
B3:=-1$
M1:=X+3$
M2:=X**2+4*X+4$
M3:=X**3+2*X+6$
M:=M1*M2*M3;
MM1:=M/M1$
MM2:=M/M2$
MM3:=M/M3$
BM:=B1*MM1+B2*MM2+B3*MM3$
ABM:=A1*B1*MM1+A2*B2*MM2+A3*B3*MM3$
G:=AMARI(BM,M)$
F:=SHO(BM,M,G-1)
YY:=F*ABM$
Y:=REMAINDER(YY,M);
END;
```

図6.　多項式環上のＲＥＤＵＣＥプログラム（高速計算法）

6．まとめ

整数環および有限体上の多項式環における中国剰余定理の解法アルゴリスムを示し，それに基づいていくつかの例を実際に計算した．第5節で述べたその計算結果から次のことが知られる．

(1) アルゴリスムの正しさが確認できた．

(2) 整数環の場合，高速計算法は通常の計算法における計算時間より，短縮できることが認められた．

(3) 多項式環においても高速計算法の計算時間は，通常の計算法におけるよりも短縮できることがわかった．

以上のように各計算法による実験結果は，長坂－Ho－Shiue の高速計算法が通常の計算法より，時間を短縮できることを実証した．

参考文献

〔1〕 Kenji Nagasaka, Jau－Shyong Shiue and Chung－Wu Ho: A Fast Algorithm of the Chinese Remainder Theorem and its Application to Fibonacci Numbers, Applications of Fibonacci Numbers, volume 4 (1991), 241－246.

〔2〕 K.H. Rosen: Elementary Number Theory and Its Application (Addison－Wesley), 1984.

〔3〕 D.E.クヌース著，中川圭介訳：The Art of Computer Programming, 4 準数値算法/算術演算．1991.サイエンス社.