Journal of Mathematical Research with Applications
Jan., 2017, Vol. 37, No. 1, pp. 90–96
DOI:10.3770/j.issn:2095-2651.2017.01.008
Http://jmre.dlut.edu.cn

Application of Polynomial Interpolation in the Chinese Remainder Problem

Tianxiao HE[1,*], Scott MACDONALD[2], Peter J.-S. SHIUE[3]

1. *Department of Mathematics, Illinois Wesleyan University, Bloomington, Illinois* 61702*, USA;*
2. *Math Learning Center, University of Nevada, Las Vegas, Las Vegas, Nevada,* 89154-1099*, USA;*
3. *Department of Mathematical Sciences, University of Nevada, Las Vegas, Las Vegas, Nevada,* 89154-4020*, USA*

Dedicated to Professor Renhong WANG on the Occasion of His Eightieth Birthday

Abstract This paper presents an application of polynomial interpolation in the solution of the Chinese Remainder Problem for bother integers and polynomials.

Keywords Chinese Remainder problem; Chinese Remainder theorem; Lagrange interpolation; Newton interpolation

MR(2010) Subject Classification 11A07; 65B10; 11A41; 33C45; 39A70; 41A80

1. Introduction

For given integers a_i $(1 \leq i \leq n)$ and positive integers m_i $(1 \leq i \leq n)$ that are pairwise relatively prime, the Chinese Remainder Problem (CRP) for integers may be stated as follows: Find an integer m satisfying the congruences

$$m \equiv a_i \pmod{m_i}, \quad i = 1, 2, \ldots, n. \tag{1}$$

Note that if we have found one solution x, then all solutions of (1) belong to its residue class modulo $M = m_1 m_2 \ldots m_n$. This result is known as the Chinese Remainder Theorem (CRT) for integers. There are numerous results on the solution of CRP, for instance, see Andrews [1], Grosswald [2], Nagasaka, Shiue, and Ho [3], etc. Particularly, an interpolation approach to the solutions can be found in Stewart [4] and surveyed in Schoenberg [5].

In this paper, we will view the solution of a CRP shown in (1) equivalently to a Lagrange interpolation or Newton interpolation, which can be used to extend the CRP for integers to the CRP for polynomials.

2. Main results

Received August 25, 2016; Accepted September 23, 2016
This work was completed while the third author is on sabbatical leave from University of Nevada, Las Vegas, and the author would like to thank UNLV for its support.
* Corresponding author
E-mail address: the@iwu.edu (Tianxiao HE); scott.macdonald@unlv.edu (Scott MACDONALD); shiue@unlv.nevada.edu (Peter J.-S. SHIUE)

We now establish the following theorem on the CRP for polynomials and view them as interpolation problems.

Theorem 2.1 *Let F be a field, and let $a_1(x)$, $a_2(x), \ldots, a_n(x)$ be arbitrary polynomials and $m_1(x), m_2(x), \ldots, m_n(x)$ pairwise relatively prime polynomials in $F[x]$. Then there exists a unique polynomial $f(x)$ such that*

$$f(x) \equiv a_i(x) \pmod{m_i(x)}, \quad i = 1, 2, \ldots, \tag{2}$$

and $\deg f(x) < \deg M(x)$, where $M(x) = \Pi_{i=1}^{n} m_i(x)$.

Proof Since $\gcd(m_i(x), m_j(x)) = 1$ for all $i \neq j$, $m_i(x)$ is relatively prime to

$$p_i(x) := \frac{M(x)}{m_i(x)}.$$

Then we can solve

$$h_i(x)m_i(x) + k_i(x)p_i(x) = 1$$

for $h_i(x)$ and $k_i(x)$. Therefore, $k_i(x)p_i(x)$ satisfies

$$\begin{aligned} k_i(x)p_i(x) &\equiv 0 \pmod{m_j(x)} \quad \text{for all} \quad j \neq i, \\ k_i(x)p_i(x) &\equiv 1 \pmod{m_i(x)}, \end{aligned}$$

or equivalently,

$$k_i(x)p_i(x) \equiv \delta_{i,j} \pmod{m_j(x)}, \tag{3}$$

where δ is the Kronecker symbol. We can use $\{k_i(x)p_i(x)\}_{i=1}^{n}$ as the Lagrange interpolation basis and construct $f(x)$ as

$$f(x) = \sum_{i=1}^{n} a_i(x)k_i(x)p_i(x). \tag{4}$$

Note that if $\deg f(x) \geq \deg M(x)$, then we can use the division algorithm to replace $f(x)$ by $r(x) = f(x) - q(x)M(x)$. □

Remark 2.2 A constructive proof of Theorem 2.1 can be found in Schroeder [6] and Bach and Shallit [7].

The proof of Theorem 2.1 gives the following algorithm based on Lagrange interpolation to solve CRP (2): (i) Set $M(x) = m_1(x)m_2(x)\cdots m_n(x)$; (ii) Solve $k_i(x)p_i(x) \equiv 1 \pmod{m_i(x)}$, where $p_i(x) = M(x)/m_i(x)$; and (iii) Write the solution of (2) as (4).

Example 2.3 As an example, we consider the CRP (A):

$$\begin{aligned} f(x) &\equiv 3 \pmod{x-1}, \\ f(x) &\equiv 2 \pmod{x-2}, \\ f(x) &\equiv -1 \pmod{x-3}. \end{aligned}$$

First, $M(x) = (x-1)(x-2)(x-3)$. Then we solve $k_1(x)$ from

$$k_1(x)\frac{M(x)}{(x-1)} \equiv 1 \pmod{x-1},$$

or equivalently,

$$k_1(x)(x-2)(x-3)+h_1(x)(x-1)=1$$

for some polynomial $h_i(x)\in F[x]$. Since

$$(x-2)(x-3)=(x-4)(x-1)+2,$$

we have

$$\frac{1}{2}(x-2)(x-3)-\frac{1}{2}(x-4)(x-1)=1,$$

which implies $k_1(x)=1/2$. Similarly, from

$$k_2(x)\frac{M(x)}{(x-2)}\equiv 1 \pmod{x-2}, \quad k_3(x)\frac{M(x)}{(x-3)}\equiv 1 \pmod{x-3},$$

we solve

$$k_2(x)=-1, \quad k_3(x)=\frac{1}{2},$$

respectively. Finally, we obtain the solution of (2)

$$f(x)=3\frac{1}{2}(x-2)(x-3)-2(x-1)(x-3)-\frac{1}{2}(x-1)(x-2)=-x^2+2x+2.$$

It is obvious that the above algorithm based on Lagrange interpolation becomes inconvenient if an extra congruence relation were included in the set of congruences that $f(x)$ must satisfy. The reason is that all $k_i(x)$ $(i=1,2,\ldots,n)$ have to be recalculated. To overcome the difficulty, we present the second method, an algorithm based on Newton interpolation, which will give an equivalent result obtained from the first method and allow to add in one more term in $f(x)$ for an extra congruence relation.

Denote by $f[x_j,x_{j+1},\ldots,x_k]$ the divided difference of f at knots $\{x_j,x_{j+1},\ldots,x_k\}$ defined by

$$f[x_j,x_{j+1},\ldots,x_k]:=\frac{f[x_{j+1},x_{j+2},\ldots,x_k]-f[x_j,x_{j+1},\ldots,x_{k-1}]}{x_k-x_j}$$

and $f[x_j]=f(x_j)$ $(1\le j<k\le n)$. Then by denoting $x_1=1$, $x_2=2$, and $x_3=3$, the solution of CRP (A) can be written as

$$f(x)=f[x_1]+f[x_1,x_2](x-x_1)+f[x_1,x_2,x_3](x-x_1)(x-x_2), \tag{5}$$

where the divided difference can be found in the following chart:

$$\begin{array}{llll} x_1=1 & f[x_1]=3 & & \\ x_2=2 & f[x_2]=2 & f[x_1,x_2]=\frac{2-3}{2-1}=-1 & \\ x_3=3 & f[x_3]=-1 & f[x_2,x_3]=\frac{-1-2}{3-2}=-3 & f[x_1,x_2,x_3]=\frac{f[x_2,x_3]-f[x_1,x_2]}{x_3-x_1}=-1 \end{array} \tag{6}$$

Thus

$$\begin{aligned} f(x)&=f[x_1]+f[x_1,x_2](x-x_1)+f[x_1,x_2,x_3](x-x_1)(x-x_2)\\ &=3+(-1)(x-1)+(-1)(x-1)(x-2)=-x^2+2x+2. \end{aligned}$$

Remark 2.4 We now compare Newton interpolation and Lagrange interpolation in the solution of CRP (A). For the view of Lagrange interpolation, we write CRP (A) as finding $f(x)$ so that

$$f(x)\equiv 3 \pmod{x-1},$$

$$f(x) \equiv 2 \pmod{x-2},$$
$$f(x) \equiv -1 \pmod{x-3},$$

which is equivalent to the interpolation problem of finding $f(x)$ so that $f(x_i) = y_i$, where $x_0 = 1$, $x_1 = 2$, $x_2 = 3$, $y_0 = 3$, $y_1 = 2$, and $y_2 = -1$. Thus, using Lagrange interpolation, we obtain

$$\begin{aligned} f(x) &= y_0 \frac{(x-x_1)(x-x_2)}{(x_0-x_1)(x_0-x_2)} + y_1 \frac{(x-x_0)(x-x_2)}{(x_1-x_0)(x_1-x_2)} + y_2 \frac{(x-x_0)(x-x_1)}{(x_2-x_0)(x_2-x_1)} \\ &= \frac{3}{2}(x-2)(x-3) - 2(x-1)(x-3) - \frac{1}{2}(x-1)(x-2) \\ &= -x^2 + 2x + 2. \end{aligned}$$

From this example, one may see if an extra congruence relation, say $f(x) \equiv 1 \pmod{x-4}$, is given, then to solve the corresponding CRP using Lagrange interpolation, each term of Lagrange interpolation needs to be reconstructed. However, Newton interpolation gives the following solution of the CRP by adding one more term in (5)

$$\begin{aligned} f(x) =& f[x_1] + f[x_1, x_2](x-x_1) + f[x_1, x_2, x_3](x-x_1)(x-x_2) + \\ & f[x_1, x_2, x_3, x_4](x-x_1)(x-x_2)(x-x_3), \end{aligned}$$

where the divided difference can be found from chart (7) by adding in one more row:

$$\begin{array}{llllll} x_1 = 1 & f[x_1] = 3 & & & & \\ x_2 = 2 & f[x_2] = 2 & f[x_1, x_2] = -1 & & & \\ x_3 = 3 & f[x_3] = -1 & f[x_2, x_3] = -3 & f[x_1, x_2, x_3] = -1 & & \\ x_4 = 4 & f[x_4] = 1 & f[x_3, x_4] = 2 & f[x_2, x_3, x_4] = 5/2 & f[x_1, x_2, x_3, x_4] = 7/6 \end{array} \tag{7}$$

Thus,

$$\begin{aligned} f(x) =& 3 + (-1)(x-1) + (-1)(x-1)(x-2) + \frac{7}{6}(x-1)(x-2)(x-3) \\ =& \frac{7}{6}x^3 - 8x^2 + \frac{89}{6}x - 5. \end{aligned}$$

Example 2.5 To show the convenience of the second method, we assume an extra congruence relation is added in CRP (A) to give the following CRP (B):

$$f(x) \equiv 3 \pmod{x-1},$$
$$f(x) \equiv 2 \pmod{x-2},$$
$$f(x) \equiv -1 \pmod{x-3},$$
$$f(x) \equiv 5 \pmod{x}.$$

Since the Newton method is independent of the order of the congruence relations, we simply input the extra relation below the congruence relations of CRP (A) and calculate the corresponding divided difference table of CRP (B) as

$$\begin{array}{llllll} x_1 = 1 & f[x_1] = 3 & & & & \\ x_2 = 2 & f[x_2] = 2 & f[x_1, x_2] = -1 & & & \\ x_3 = 3 & f[x_3] = -1 & f[x_2, x_3] = -3 & f[x_1, x_2, x_3] = -1 & & \\ x_4 = 0 & f[x_4] = 5 & f[x_3, x_4] = -2 & f[x_2, x_3, x_4] = -\frac{1}{2} & f[x_1, x_2 x_3 x_4] = -\frac{1}{2} \end{array}$$

Thus the solution of CRP (B) is

$$\begin{aligned} f(x) =& f[x_1] + f[x_1, x_2](x - x_1) + f[x_1, x_2, x_3](x - x_1)(x - x_2) + \\ & f[x_1, x_2, x_3, x_4](x - x_1)(x - x_2)(x - x_3) \\ =& 3 + (-1)(x - 1) + (-1)(x - 1)(x - 2) + \big(-\frac{1}{2}\big)(x - 1)(x - 2)(x - 3) \\ =& -\frac{1}{2}x^3 + 2x^2 - \frac{7}{2}x + 5. \end{aligned}$$

We now survey the Newton interpolation method for CRP as follows.

Theorem 2.6 *Let F be a field, and let $\{a_i\}_{i=1}^n \in F$ and distinct $\{b_i\}_{i=1}^n \in F$. Then there exists a unique polynomial $f(x) \in F[x]$ with degree $< n$ such that*

$$f(b_i) = a_i \tag{8}$$

for $i = 1, 2, \ldots, n$, which is equivalent to

$$f(x) \equiv a_i \pmod{x - b_i} \tag{9}$$

for $i = 1, 2, \ldots, n$.

Proof Denote $m_i(x) = x - b_i$ and $a_i(x) = a_i$. Then Theorem 2.1 guarantees the unique existence of $f(x)$ that satisfies (9). The equivalence between (9) and (8) from the fact that $f(x) \equiv a_i \pmod{x - b_i}$ is equivalent to $f(b_i) = a_i$ for $i = 1, 2, \ldots, n$. □

Besides the convenience to treat extra congruence relations, from the following examples we shall see the computation derived from Theorem 2.6 is simpler than the method from 2.1 usually. As an example, one may see Example 2.7 below.

The above example works for linear congruence relations. We now give a general description of the algorithm based on Newton interpolation for arbitrary congruence relations of the CRP (2), that is, to find $f_1 \equiv f_1(x)$, $f_2 \equiv f_2(x), \ldots$ successively from the following congruence system:

$$\begin{aligned} f_1 &\equiv a_1(x) \pmod{m_1(x)}, \\ f_1 + f_2 m_1 &\equiv a_2(x) \pmod{m_2(x)}, \\ f_1 + f_2 m_1 + f_3 m_1 m_2 &\equiv a_3(x) \pmod{m_3(x)}, \\ &\cdots, \\ f_1 + f_2 m_1 + \cdots + f_n m_1 m_2 \cdots m_{n-1} &\equiv a_n(x) \pmod{m_n(x)}. \end{aligned}$$

Then the solution $f(x)$ of CRP (2) is

$$f(x) = f_1 + f_2 m_1 + \cdots + f_n m_1 m_2 \cdots m_{n-1}.$$

Indeed, for each $i = 1, 2, \ldots, n$,

$$f(x) = f_1 + f_2 m_1 + \cdots + f_i m_1 m_2 \cdots m_{i-1} \pmod{m_i} = a_i(x) \pmod{m_i},$$

which is from the congruence system.

Example 2.7 Consider the following CRP (C) with nonlinear congruence relations

$$f(x) \equiv x - 1 \pmod{x^2 - x + 1},$$
$$f(x) \equiv x \pmod{x - 1}.$$

Solving the corresponding congruence system:

$$f_1 \equiv x - 1 \pmod{x^2 - x + 1},$$
$$f_1 + f_2(x^2 - x + 1) \equiv x \pmod{x - 1},$$

we may obtain $f_1(x) = x - 1$ and $f_2(x) = 1$. Thus the solution of CRP (C) is

$$f(x) = x - 1 + 1 \cdot (x^2 - x + 1) = x^2.$$

Using Theorem 2.6, we may find $f(x)$ more easily. In fact, from $f_1(x) = x - 1$, we have

$$x - 1 + f_2(x^2 - x + 1) \equiv x \pmod{x - 1},$$

or equivalently,

$$-1 + f_2(x^2 - x + 1) \equiv 0 \pmod{x - 1},$$

which, from Theorem 2.6, is equivalent to

$$-1 + f_2(x^2 - x + 1)\big|_{x=1} = 0.$$

Hence, $f_2(x) = 1$ and $f(x) = x - 1 + (x^2 - x + 1) = x^2$.

Sometimes, we may find the mixed method derived from Theorems 2.1 and 2.6 might be more convenient in solving division problems. We use the following example to demonstrate this mixed method.

Example 2.8 ([8, P.124]) Let $p(x)$ be a polynomial satisfying the conditions that if it is divided by $(x - 2)^2$ and $2x - 1$, then remainders $56x - 42$ and 5 are obtained. To find the remainder when $p(x)$ is divided by $(x - 2)^2(2x - 1)$, we denote

$$p(x) = q_1(x)(x - 2)^2 + 56x - 42, \quad p(x) = q_2(x)(2x - 1) + 5$$

for some $q_1(x)$ and $q_2(x)$. Then, we obtain the following CRP:

$$p(x) \equiv 56x - 42 \pmod{(x - 2)^2}, \quad p(x) \equiv 5 \pmod{2x - 1}.$$

From Theorem 2.1, we have

$$f_1(x) \equiv 56x - 42 \pmod{(x - 2)^2}, \quad f_1(x) + f_2(x - 2)^2 \equiv 5 \pmod{2x - 1},$$

which implies

$$56x - 42 + f_2(x - 2)^2 \equiv 5 \pmod{2x - 1}.$$

From Theorem 2.6, we have

$$56\left(\frac{1}{2}\right) - 42 + f_2\left(\frac{1}{2}\right)\left(\frac{1}{2} - 2\right)^2 = 5,$$

which implies $f_2 = 76/9$ and

$$p(x) = 56x - 42 + \frac{76}{9}(x-2)^2 = \frac{1}{9}(76x^2 + 200x - 74).$$

References

[1] G. E. ANDREWS. *Number Theory*. Dover Publications, Inc., New York, 1994.
[2] E. GROSSWALD. *Topics from the Theory of Numbers*. Reprint of the 1984 second edition. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2009.
[3] K. NAGASAKA, P. J.-S. SHIUE, C.-W. HO. *A Fast Algorithm of the Chinese Remainder Theorem and its Application to Fibonacci Numbers*. Kluwer Acad. Publ., Dordrecht, 1991.
[4] B. M. STEWART. *Theory of Numbers*. Second Edition, The Macmillan Co., New York; Collier-Macmillan Ltd., London 1964.
[5] I. J. SCHOENBERG. *The Chinese remainder problem and polynomial interpolation*. College Math. J., 1987, **18**(4): 320–322.
[6] M. R. SCHROEDER. *Number Theory in Science and Communications*. Second Enlarged Edition, Springer-Verlag, 1985.
[7] E. BACH, J. SHALLIT. *Algorithmic Number Theory*. Vol. 1. Efficient algorithms. Foundations of Computing Series. MIT Press, Cambridge, MA, 1996.
[8] R. S. MILLMAN, P. J. SHIUE, E. B. KAHN. *Problems and Proofs in Numbers and Algebra*. Springer, Cham, 2015.