British Journal of Mathematics & Computer Science
8(3): 265-273, 2015, Article no.BJMCS.2015.160
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Current Development of Historical Methods for Solving Linear Systems of Simultaneous Congruences

Yang Liu[1] and Robert Goutte[2*]

[1]Shanghai Medical Instrumentation College, 101 Yingkou Road, Yangpu District 200093, Shanghai, China.
[2]University of Lyon, INSA, labo CREATIS, Umr Cnrs 5220, Inserm 1044, Lyon, France.

Article Information

DOI: 10.9734/BJMCS/2015/16683
Editor(s):
(1) Dijana Mosi´c, Department of Mathematics, University of Niˇs, Serbia.
Reviewers:
(1) Grienggrai Rajchakit, Mathematics Department, Maejo University, Thailand.
(2) Anonymous, Mexico.
Complete Peer review History: http://www.sciencedomain.org/review-history.php?iid=1032&id=6&aid=8698

Short Communication

Received: 10 February 2015
Accepted: 02 March 2015
Published: 06 April 2015

Abstract

Based on the very old methods of solving linear systems of simultaneous congruences, the Chinese Remainder Theorem is still an irreplaceable tool in Computing, Signal Processing and Information security.

We demonstrate its potential by considering an example of an application concerning quaternionic imaging.

Keywords: Chinese remainder theorem; congruences; quaternionic imagery.

1 Introduction

In the first century AD, a Chinese mathematician by the name of SUN ZI, published a book, Sun Zi Suanjing, or the Arithmetical Classic of Sun Zi [1]. In this book Sun Zi introduced a method for solving linear systems of congruences (cf Annex 1) that is known as the Chinese Remainder Theorem, or CRT [2].

Republished in 1247(AD) by Qin Jiushao, CRT has become, in the last thirty years of our modern era ,an irreplaceable tool used in computing, signal processing and information security.

**Corresponding author: robert.goutte@creatis.insa-lyon.fr;*

2 Historical Development

Sun ZI (or Sun Tzu) was a Chinese mathematician and astronomer who lived between the 3rd and 5th centuries, during the Wei and Jin dynasties. Interested in astronomy and with a desire to develop a calendar, he investigated Diophantine equations. He is known primarily as the author of a book, SunZi Suan Jing, or the "Arithmetical Classic of SunZI", which contains the earliest known example and the formulation of the famous "Chinese Remainder Theorem", or CRT. The results concerning a general method for solving the linear systems of congruences were published for the first time, much later, in 1247 by Quin Jiushao.

Aryabhata, (476-550), Hindu Mathematician, published his work about a century after Sun Zi Suanjing and invented a general rule for solving undetermined equations (a method called KUTTAKA).

During the 11th century, **Ibn Tahir** (sometimes known as **Al-Baghadi**), 980-1039, used the CRT in his treatise Al Takmila.

Fibonacci (1170-1250) was the first European to study the CRT in his Liber Abaci, in 1202.

Quin Jiushao (1202-1261) was one of the greatest mathematicians in Chinese history. He composed the great work Mathematical Treatise in Nine Sections. The work included the Dayan General Mathematical Art, a general form of the Chinese Remainder Theorem solution of linear congruences equation and the algorithms to solve it. He also introduced the zero symbol into written Chinese mathematics.

Later during the 14th and 15th centuries, **Isaac Argyros** and **Frates Federicus** used the CRT in their treatise Eisagoges Arithmetike.

Leonard Euler (1707-1783) gave the general solution for solving linear systems of congruences (Euler theorem).

Friedrich Gauss (1777-1855) published, in 1801, his book Disquisitiones Arithmeticae of which several chapters are devoted to equivalence and solvability of congruences.

3 Base of Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) is mainly based on the algorithm of linear congruencies. The system of linear congruencies $a \cong b \pmod{m}$ can be reduced to a set of $a \cong b_i \pmod{m_i}$, with: $1 \le i \le k$

$$x \cong [a_1M_1y_1 + a_2M_2y_2 + \cdots + a_kM_ky_k](\mathrm{mod}\ M)$$

with $M = m_{1\,x}\, m_{2\,x} \cdots {}_x\, m_k$, $M_i = M/m_i$,

$y_i \cong (M_i)^{-1} (\mathrm{mod}\ m_i)$ and y_i integer which verifies: $y_i\, M_i \cong 1 (\mathrm{mod}\ m_i)$.

(Two numbers are considered to be relatively prime if their greatest common divisor is 1).

If the equation set does not meet the restrictions (no coprimes) to be solved by the traditional CRT method, then the algorithm should convert it to a new set of equations, where the moduli are relatively prime.

4 Historical Example of Problem

An old woman goes to the market with a basket of eggs. She sets the basket down and a horse accidentally steps on it, crushing all the eggs. The rider offers to pay her for the damaged eggs and asks how many eggs she had. She tells the rider that she can't remember but that when she took all of the eggs out, three at a time, there were two left in the basket. When she took them out five at a time, there were three left and when she took them out seven at a time, there were two left.

What is the smallest number of eggs she could have had?

In this example we have a system of three simultaneous congruences

Congru1 $x \cong 2 \pmod 3$
Congru2 $x \cong 3 \pmod 5$
Congru3 $x \cong 2 \pmod 7$

5 Solution (with Sun ZI algorithm)

The Chinese Remainder Theorem (CRT) is mainly based on the algorithm of linear congruencies. The system of linear congruencies $a \cong b \pmod m$ can be reduced to a set of $a \cong b_i \pmod {m_i}$, with: $1 \le i \le k$. (Cf Annex1).

If the equation set does not meet the restrictions (not coprimes) to be solved by the traditional CRT method, then the algorithm should convert it to a new set of equations, where the modules are relatively prime.

(Two numbers are considered to be relatively prime if their greatest common divisor is 1).

$x \cong [a_1M_1y_1 + a_2M_2y_2 + \cdots + a_kM_ky_k] \pmod M$ with $M = m_1 \times m_2 \times \cdots \times m_k$, $M_i = M/m_i$, $y_i \cong (M_i)^{-1} \pmod {m_i}$ and y_i integer which verifies: $y_i M_i \cong 1 \pmod {m_i}$.

$m_1=3$ $m_2=5$ $m_3=7$ $M=3x5x7=105$

$a_1=2$ $a_2=3$ $a_3=2$ $M_1=35$ $M_2=21$ $M_3=15$

$y_i \cong (M_i)^{-1} \pmod {m_i} \rightarrow y_1 \cong (35)^{-1} \pmod 3 = 2$

$y_2 \cong (21)^{-1} \pmod 5 = 1$ $y_3 \cong (15)^{-1} \pmod 7 = 1$

We obtain: $x=[2X35X2+3X21X1+2X15X1](mod105)=233(mod105)=$**23**

5.1 Other Method

We convert the three congruences into sets and write the elements out to the product

$M=3X5x7=105$

With congr 1 : x=(2,5,8,11,14,17,20,**23**,26,29,32,35,.., 98,101,104,……
With congr 2 x=8,13,18,**23**,2833,38,43,53,58,63,68,73,78,83,88,93,98,103,…
With congr 3 x=(2,9,16,**23**,30,37,44,51,58,65,72,79,86,93,100,……

To find an x that satisfies all three congruences, intersect the three sets to get:

x=23 (mod 105) or x**=23**+105 u, with u= 0, 1, 2 ,…∞.

6 The Inverse CRT

The objective of the inverse CRT is to represent any integers x $(0 < x < M-1)$ with a set of integers a_i function of m_1, m_2,…m_K. The a_i are obtained from the following set of simultaneous congruences.

$a_{i} \cong x(\text{mod } m_{i)}$.

We have with the preceding examples: X=23

with $m_1=3$, $m_2=5$, $m_3=7$

$a_1=23(\text{mod}3)$, $a_2=23(\text{mod}5)$, $a_3=23(\text{mod}7)$
$a_1=2$ $a_2=3$ $a_3=2$

So, from the free values 3, 5, 7 of the common key and with the final value 23 (compressed information), we can rediscover the three initial values $a_{i\,:}$ 2, 3; 2.

7 Philosophy

The Chinese Remainder Theorem can be viewed as a manifestation of the general principle “pars pro toto” - a part goes for the whole thing.

The CRT is basically a divide-and-conquer technique. The original problem given problem is divided into sub problems. The latter can be solved independently of each other, and then combined in parallel, giving the original problem. **It is amazing to see how ancient mathematics like the CRT and Euclidian algebra, have continued to find many applications today!**

(A Google search using the search term “Chinese Remainder Theorem” gives more than 390000 results!).

8 Applications of the CRT

The Chinese Remainder Theorem has applications in many fields, the main ones being computing, coding theory, cryptography and signal processing.

The advantages to CRT approach for computing are that it requires less memory size and computation time. This result is obtained by its use parallelization and simple arithmetic operations.

In coding theory, detection and correction of errors is carried out by adding redundancy to data that is sent via a noisy channel or in a computer. The CRT remainder techniques are useful in developing code that detects errors.

In cryptography, the CRT is used in secret sharing through error-correcting code. The CRT is itself a secret-sharing scheme without any need for modification: The CRT is itself a secret-sharing scheme without any need for modification.

The CRT gave rise to modular technique for signal and image processing. Cyclic convolution and Fourier transform are important elements of digital signal processing.

To illustrate the potential of CRT in image processing we propose an unconventional application in quaternion spectral imagery.

9 Quaternionic Fourier Transform

Based on the quaternion's concept, the QFT has been introduced by Ell [3]. The quaternion Fourier Transform of a 2D real signal f(x, y) is defined as:

$$\mathrm{F_q}(\mathrm{u},\mathrm{v}) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \mathrm{e}^{-\mathrm{i}2\pi\mathrm{ux}}\mathrm{f}(\mathrm{x},\mathrm{y})\mathrm{e}^{-\mathrm{j}2\pi\mathrm{vy}}\,\mathrm{dx}\,\mathrm{dy}$$

This QFT, of type 1 [4,5] is noted two-side. If the input f(x, y) is a quaternion function and not only a real function [5]; we can decompose f(x, y) as:

$$\mathrm{f}(\mathrm{x},\mathrm{y}) = \mathrm{f_r}(\mathrm{x},\mathrm{y}) + \mathrm{f_i}(\mathrm{x},\mathrm{y})\cdot\mathrm{i} + \mathrm{f_j}(\mathrm{x},\mathrm{y})\cdot\mathrm{j} + \mathrm{f_k}(\mathrm{x},\mathrm{y})\cdot\mathrm{k}$$

where f_r(x, y), f_i(x, y), f_j(x, y) and f_k(x, y) are real functions. We obtain:

$$\mathrm{F_q}(\mathrm{u},\mathrm{v}) = \mathrm{F_{rq}}(\mathrm{u},\mathrm{v}) + \mathrm{F_{iq}}(\mathrm{u},\mathrm{v})\mathrm{i} + \mathrm{F_{jq}}(\mathrm{u},\mathrm{v})\mathrm{j} + \mathrm{F_{kq}}(\mathrm{u},\mathrm{v})\mathrm{k}$$

The QFT is invertible and its inverse is expressed as:

$$f(x,y) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} e^{i2\pi ux}F_q(u,v)e^{j2\pi vy}\,du\,dv$$

The discrete Quaternion Fourier Transform (DQFT) was introduced by Sangwine and Ell in year 2000. This transform has many different expression types .In this paper; we only use the type 1 of DQFT, which has the following expression (direct formulation):

$$F_q(u,v) = \sum_{M=0}^{M-1}\sum_{N=0}^{N-1} e^{-i2\pi\left(\frac{xu}{M}\right)}f(x,y)e^{-i2\pi\left(\frac{yv}{N}\right)}$$

10 CRT and Quaternionic Spectral Imagery

A real 2D image B/W: f(x,y) is considered (Fig. 1). Its spectrum (Fig. 2), is computed with the Quaternion Fourier Transform (QFT). The reversible spectrum obtained Fq(u,v) is a quaternion.

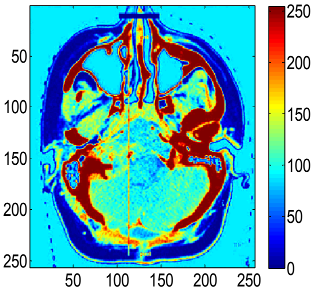

Fig. 1. Original image

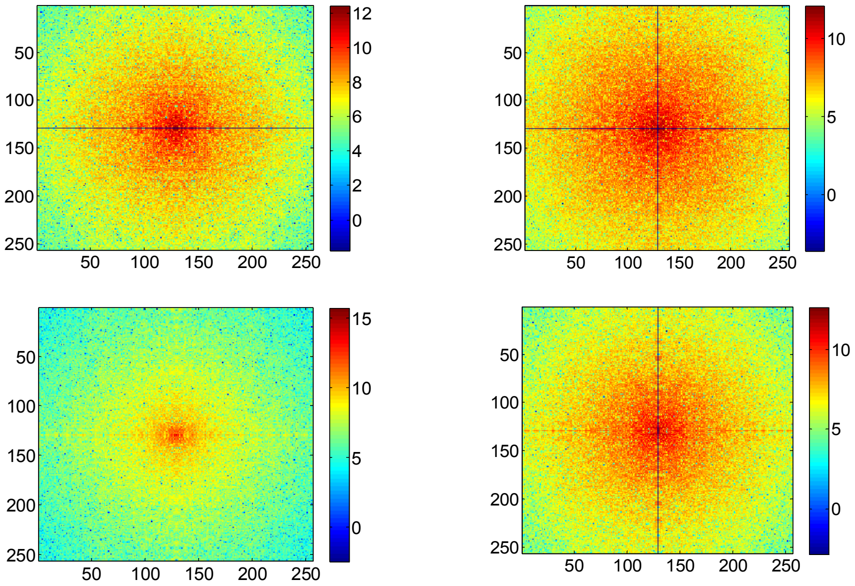

Fig. 2. Spectrum (r,i,j,k)

Given the Hermitian symmetry [6], we retain only (Fig. 3) the for spectrum of the first quadrant $\Gamma_q(u,v)$.

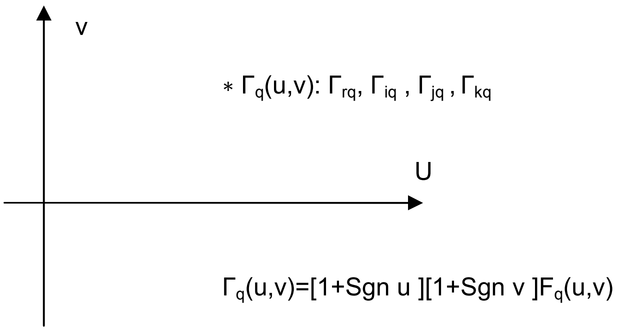
v
$* \Gamma_q(u,v)$: Γ_{rq}, Γ_{iq} , Γ_{jq} , Γ_{kq}
U
$\Gamma_q(u,v)=[1+\text{Sgn } u][1+\text{Sgn } v]F_q(u,v)$

Fig. 3. Quaternionic spectrum

With B/W we obtain four tables (u,v) : real, i ,j ,k with 4×(N×M) pixels of eight bits. For each value of u,v we obtain one block 2x2 of 8 bits which corresponds to a total of 32 bits .

Example: Block 2x2 belonging to the for components of the spectrum

235	135
156	223

But 235=14×16+11, 135=8×16+7, 156=9×16+12, 223=13×16+15. We obtain a block 4x2 in four bits coding after division by 16:

14	8	9	13
11	7	12	15

10.1 Selection of the Key

We choose the eight prime numbers: 2 3 5 7 11 13 17 19 (The key can be obtained after a random selection). We obtain eight simultaneous congruences:

x= 14 mod 2
x=11 mod 3
x= 8 mod 5
x= 7 mod 7

x=9 mod11
x=12 mod13
x=13 mod17
x=15 mod 19

The solution in decimal notation [7], is 6354698, which corresponds to the 23 bits followings: 11000001111011100001010.

The compression is lossless and the ratio is 32/23=1, 39. (For a particular data set, the values of the key components can be optimized, as well as their classification).

With a complementary Huffman encoding, we obtain 201701 in decimal notation and only 110001001111100101 in binary notation (18 bits). The total ratio of compression is then: 18/32=56/100. (In this case, the use of compression by Gödelization is not very interesting, because our previous value: 6354698 is already a prime number and the decomposition in prime factors is irrelevant).

This compression [8] is possible due to the non-random nature of the spectral data. In the absence of redundancy in the data, no compression is possible!

If the real original image is a color image RGB, we process the three components independently, as three images B/W.

11 Interpretation

The results obtained with a single key are not constant and are based on statistical properties of the data redundancy We chose this example of application because it corresponds to the general approach of the CRT, which realizes the grouping of the quaternionic spectrum, divided into four components r, i, j, k in a unique spectrum. This spectrum is solution of system congruence, associated with these four spectral components.

The compression via CRT is subject to severe constraints that limit performance. Indeed, in this application, the key must be unique and, in these circumstances, cannot adapt to local conditions. If this unicity condition was not satisfied, it would be necessary to transmit all the keys used, which would lead to the disappearance of any compression. Furthermore, the compression ratio is dependent to choice of the key.

12 Conclusions

The use of the CRT in image compression is mainly justified by the potential insertion of coded information (digital watermarking, RSA cryptosystem). In pure compression, a performance remains modest and limits the diffusion of this method.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Kangsheng Shen. Archive for History of Exact Sciences. 1988;38(4):285-305.

[2] Ding C, Pei D, Salomaa A. Chinese remainder theorem. World Scientific Publishing, Co Pte. Ltd; 1996.

[3] Ell TA. Hypercomplex spectral transforms. PhD Thesis, Université of Minnesota; 1992.

[4] Pei SC, Ding JJ, Chang JH. Efficient implementation of quaternion Fourier transform. IEEE Transactions on Signal Processing. 2001;49(11):2783-2797.

[5] Girard R, Pujol PC, Clarysse A.Marion, Goutte R, Delachartre P. Analytic video signal by clifford fourier transform. 9th Int Conf on Clifford Algebra, Weimar, Germany. 2011;7.

[6] Hahn SL. Multidimensional complex signals with single- orthant. IEEE Proceeding. 1992;80:1287-1300.

[7] Davidwees.com. Chinese remainder theorem, Calculator this calculate the smallest solution of a list of modulo equations.

[8] Yang Liu, Robert Goutte. Lossy and lossless spectral image compression using Quaternion Fourier Transform, 11th IEEE Int Conf on Signal Processing, ICSP, Beijing; 2012.

ANNEX I

Congruence (Latin congruentia: consistency, Accordance)

Congruence on the integers is a relationship between two integers. It is the foundation of modular arithmetic.

Congruence modulo m.

Two integers a and b are called congruent modulo m (where m, modulus, is a strictly positive integer greater than or equal to 2), if one of these two equivalent conditions is satisfied.

1) Their difference is divisible by m.

   a-b= *k* m *k* integer

2) The remainder (or residue) of the Euclidean division of a by m is equal to that of the division of b by m.

   Notation: a≅ b (mod m)

Properties

Reflectivity: a≅a(mod m)

Symmetry: if a≅b(mod m) then b≅ a(mod m)

Transitivity: if a≅b(mod m) and b≅c(mod m)

then a≅c(mod m)

© 2015 Liu and Goutte; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
www.sciencedomain.org/review-history.php?iid=1032&id=6&aid=8698