数理解析研究所講究録
第708巻 1989年 1-10

A FAST ALGORITHM
OF
THE CHINESE REMAINDER THEOREM

BY

Kenji Nagasaka (Univ. of the Air, Chiba, Japan)
Jau-Shyong Shiue (Univ. of Nevada, Las Vegas, U.S.A.)
Chung-Wu Ho (Southern Illinois Univ., Edwardsville, U.S.A.)

0. Background Information

In the first century A.D. the chinese scholar Sun-Tzu authored a book which contained an obscure verse called t'ai-yen (great generalization) to determine a number having remainder 2, 3 and 2 when divided by 3, 5 and 7, respectively.

This result was apparently first stated as a theorem and proved in its proper generality by L. Euler in 1734, although a description of most of the necessary principles was given in China by Chhin Chiu-Shao in his Shu Shu Chiu Chang in 1247) [1],[2],[3].

The Chinese Remainder Theorem. *Let* $m_1, m_2, \cdots, m_k$ *be positive integers which are relatively prime in pairs. Then there exists a unique integer* $x \bmod M$ *satisfying the system of congruences:*

$$(0.1) \qquad \begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \cdots \quad \cdots \\ x \equiv a_k \pmod{m_k}, \end{cases}$$

where $M = m_1 m_2 \cdots m_k$.

Proof. We prove first the uniqueness of the solution of (0.1) mod M. Suppose x and y to be solutions of (0.1). That is, for $i = 1, 2, \cdots, k$,

$$x \equiv a_i \pmod{m_i},$$

and

$$y \equiv a_i \pmod{m_i} .$$

Then, for $i = 1, 2, \cdots, k$,

$$x \equiv y \pmod{m_i} ,$$

from which we derive

$$x - y \equiv 0 \pmod{m_i}$$

for $i = 1, 2, \cdots, k$. Thus $x - y$ is a multiple of m_i for all i, so the pairwise coprime moduli asserts that $x - y$ is a multiple of $M = m_1 m_2 \cdots m_k$, which signifies the uniqueness of the solution of (0.1).

To complete the proof, we must only show the existence of at least one solution.

The first proof of the existence can be done by nonconstructive way. There exist exactly M k-tuples $(u_1, u_2, \cdots, u_k)$ of integers with $0 \leqq u_i \leqq m_i - 1$, for $i = 1, 2, \cdots, k$. As an integral variable x runs through the M distinnct values $0 \leqq x \leqq M-1$, the k-tuples

$$(x \bmod m_1, x \bmod m_2, \cdots, x \bmod m_k)$$

must also run through M distinct values, since (0.1) has at most one solution mod M. Therefore each k-tuple must occur exactly once, and there must be some value of x for which

(0.2) $$(x \bmod m_1, x \bmod m_2, \cdots, x \bmod m_k) = (a_1, a_2, \cdots, a_k) .$$

The second proof of the existence is constructive. Let us define, for $i = 1, 2, \cdots, k$,

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

and put

(0.3) $$y_i = M_i^{\varphi(m_i)} ,$$

for $i = 1, 2, \cdots, k$. Then the Fermat's little theorem shows

$$y_i \equiv 1 \pmod{m_i} ,$$

since M_i and m_i are coprime. We have also

$$y_i \equiv 0 \pmod{m_j} ,$$

for all $j \neq i$. Now the number

$$x = a_1y_1 + a_2y_2 + \cdots + a_ky_k$$

is a solution of the system of congruences (0.1).

<Q. E. D.>

Remark 0-1. In order to check whether (0.2) holds or not for a special value of x , we need one time tuple-wise subtraction. The number of necessary tuple-wise subtraction is at most $Mk/(\max_i m_i)$.

Remark 0-2. Instead of putting y_i as in (0.3), we can find a unique solution $z_i \bmod m_i$ satisfying the congruence

$$M_iz_i \equiv 1 \pmod{m_i} , \tag{0.4}$$

for $i = 1, 2, \cdots, k$. In order to obtain a particular solution of (0.4), we consider the linear diophantine equation

$$M_ix - m_iy = 1 . \tag{0.5}$$

Since M_i and m_i are relatively prime, the Euclidean algorithm to find the greatest common divisor gives a solution of (0.5). The number of divisions needed to find the greatest common divisors of two positive integers using the Euclidean algorithm does not exceed five times the number of digits in the smaller of the two integers, which is known as a Lamé's theorem [2]. Thus we need at most $5 \log_{10}\{\min(M_i, m_i)\}$ times divisions. Then at most $2\times5 \log_{10}\{\min(M_i, m_i)\}$ times multiplications and $5 \log_{10}\{\min(M_i, m_i)\}$ times additions give the solution of (0.5).

1. Fast Algorithm of the Chinese Remainder Theorem

In this Section, we state our theorem with full proof and show the efficiency of it.

Theorem 1. *Under the same assumptions as in the Chinese Remainder Theorem, the system of congruences* (0.1) *is equivalent to the following single linear congruence*

$$(1.1) \qquad (\sum_{i=1}^{k} b_i M_i)x \equiv \sum_{i=1}^{k} a_i b_i M_i \pmod{M} ,$$

where b_i's *are arbitrary integers coprime to* m_i's , *respectively, and* $M_i = M/m_i$ *for* $i = 1, 2, \cdots, k$ *with* $M = \prod_{i=1}^{k} m_i$.

Lemma 1. *The system of congruences* (0.1) *is equivalent to the following system of congruences:*

$$(1.2) \qquad \begin{cases} M_1 x \equiv a_1 M_1 \pmod{M} \\ M_2 x \equiv a_2 M_2 \pmod{M} \\ \quad \cdots \\ M_{k-1} x \equiv a_{k=1} M_{k-1} \pmod{M} \\ (\sum_{i=1}^{k} b_i M_i)\, x \equiv \sum_{i=1}^{k} a_i b_i M_i \pmod{M} , \end{cases}$$

where b_i *is relatively prime to* m_i *for* $i = 1, 2, \cdots, k$.

Proof of Lemma 1. We show the necessity. Suppose x to be a solution of (0.1). Then, for $i = 1, 2, \cdots, k$,

$$x - a_i = c_i m_i ,$$

with an integer c_i . Multiplying M_i with the above identity, we get, for $i = 1, 2, \cdots, k$.

$$M_i x - M_i a_i = c_i m_i M_i = c_i M ,$$

which is rewritten to the congruence

(1.3) $$M_i x \equiv M_i a_i \pmod{M}$$

for $i = 1, 2, \cdots, k$. The first $k - 1$ congruences in (1.2) are identical with those of (1.3) for $i = 1, 2, \cdots, k-1$. The last congruence of (1.2) can be obtained as a linear combination of (1.3).

Conversely, we assume that x is a solution of the system of congruences. Since M_i and m_i are coprime, (1.3) can be reduced to

$$x \equiv a_i \pmod{m_i} ,$$

for $i = 1, 2, \cdots, k-1$.

Subtracting the linear combination of the first $k - 1$ congruences in (1.2), we have

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

Since M_k and b_k are relatively prime to m_k , we conclude that

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

<Q. E. D. of Lemma 1>

Lemma 2. *Under the same assumptions as in Theorem 1 and in Lemma 1,* M *is relatively prime to* $\sum_{i=1}^{k} b_i M_i$.

Proof of Lemma 2. Let g be the greatest common divisior of $\sum_{i=1}^{k} b_i M_i$ and M and let p be a prime factor of g . Then p divides $\sum_{i=1}^{k} b_i M_i$ and $M = \prod_{i=1}^{k} m_i$. The divisibility of M by p asserts that p divides only one of m_i , say m_j , since $(m_i, m_j) = 1$ if $i \neq j$. Then p divides all M_i but M_j , since $M_j = M/m_j$. Together with the divisivility of $\sum_{i=1}^{k} b_i M_i$ by p , we derive that p divides $b_j M_j$ and consequently divides b_j . Hence p divides the greatest common divisor of m_j and b_j which is equal to one from the assumption.

<Q. E. D. of Lemma 2>

Proof of Theorem 1. By Lemma 1, we know that the system of congruences (0.1) is equivalent to the system (1.2). From Lemma 2, the last congruence has a unique solution, say $x_0 \bmod M$. Thus the system (1.2) has a unique solution x_0, which implies that x_0 is the unique solution of the system of congruences (0.1), since the chinese remainder theorem assures the unique existence of the system (0.1) $\bmod M$.

<Q. E. D. of Theorem 1>

Now we can roughly estimate the number of arithmetical operations as in the arguments of Remark 0-2. We may assume that the moduli m_i's are d digits positive integers, so that the number of digits of M_i is roughly $(k - 1)d$ and obviously $\min(M_i, m_i) = m_i$, for $i = 1, 2, \cdots, k$. To get the final solution $\bmod M$ of (0.1), we need at most $5kd$ times divisions, $(10d + 1)k$ multiplications and $(5d + 1)k$ additions.

Since we can set b_i's in Theorem 1 to be ± 1, $\sum_{i=1}^{k} b_i M_i$ can be small of the order of one M_i, if k is odd. In this case, to get the solution $\bmod M$ of (1.1), we need at most $5kd - 5d$ times divisions, $(10d + 1)k - 10d$ multiplications and $(5d + 2)k - d$ additions.

As we will see in the next Section, the choice of m_i's and the number of moduli are fairly arbitrary. Thus $\sum_{i=1}^{k} b_i M_i$ can be small, which gives the advantage of the methods based on our Theorem 1.

2. Application of the Chinese Remainder Theorem

The chinese remainder theorem provides a way for doing arithmetic on large integers. Let $m_1, m_2, \cdots, m_k$ be positive integers which are relatively prime in pairs. Instead of doing arithmetics directly to an integer x, we consider the k-tuple of residues of $x \bmod m_i$. That is, for an integer $x \bmod M$, we can correspond the k-tuple of residues:

$$(x \bmod m_1,\ x \bmod m_2,\ \cdots,\ x \bmod m_k)\ ,$$

where $M = \prod_{i=1}^{k} m_i$. This correspondence is one to one due to the chinese remainder theorem. For convenience, we write this correspondence as follows:

$$x \leftrightarrow (x_1, x_2, \cdots, x_k)\ , \tag{2.1}$$

where $x_i \equiv x \pmod{m_i}$, for $i = 1, 2, \cdots, k$. We call $(x_1, x_2, \cdots, x_k)$ in (2.1) a *modular representation* of the integer x .

A modular representation allows us to do arithmetic of large integers with computers of small word-size. Addition, subtraction and multiplication of a modular representation are defined by:

$$(x_1, \cdots, x_k) + (y_1, \cdots, y_k) = ((x_1 + y_1) \bmod m_1, \cdots, (x_k + y_k) \bmod m_k)\ ,$$

$$(x_1, \cdots, x_k) - (y_1, \cdots, y_k) = ((x_1 - y_1) \bmod m_1, \cdots, (x_k - y_k) \bmod m_k)\ ,$$

$$(x_1, \cdots, x_k) \times (y_1, \cdots, y_k) = ((x_1 \times y_1) \bmod m_1, \cdots, (x_k \times y_k) \bmod m_k)\ .$$

The process of addition, subtraction and multiplication using the above definitions is called *residue arithmtic* or *modular arithmetic* and the chinese remainder theorem affords, the usual values of $x + y$, $x - y$, $x \times y$ mod M[2].

The range of integers that can be handled by modular arithmetic is equal to $M = \prod_{i=1}^{k} m_i$ and the multiplication of n-digit numbers by modular arithmetic is essentially proportional to n (not counting the time to convert in and out of representation). On the contrary the conventional multi-precision multiplication requires an execution time proportional to n^2 [2].

Furthermore the operations with respect to different moduli can all be done at the same time by using pararell computers, which gives a significant advantage of modular arithmetic also for addition and subtraction.

On most computers the word size is a large power of 2 , with 2^{35} a

common value. We pick 6 moduli, $m_1 = 2^{35} - 1$, $m_2 = 2^{34} - 1$, $m_3 = 2^{33} - 1$, $m_4 = 2^{31} - 1$, $m_5 = 2^{29} - 1$, and $m_6 = 2^{25} - 1$. Since the exponents of 2 in the expressions for the m_i's are relatively prime, then m_i's are relatively prime. Then we can do arithmetic with integers as large as 2^{186}, since $M = \prod_{i=1}^{6} m_i > 2^{186}$. We have also

$$m_1 - m_2 - m_3 + m_4 + m_5 - m_6 = 2^{25} \cdot 175 < 2^{34} - 1 = m_2 ,$$

which shows an advantage of our Theorem 1 explained at the end of the last Section for getting the solution of the system of congruences (0.1) via the only single linear congruence (1.1).

3. Generalizations and Concluding Remarks

We recall the generalized chinese remainder theorem [3].

The Generalized Chinese Remainder Theorem. *A necessary and sufficient condition that the system of congruences* (0.1) *be solvable is that, for each* $1 \leq i < j \leq k$,

$$a_i - a_j \equiv 0 \pmod{(m_i, m_j)} .$$

Any two solutions are congruent $\bmod[m_1, m_2, \cdots, m_k]$, *where* $[a, b]$ *denotes the least common multiple of two positive integers* a *and* b.

Proof. We show first the necessity. If the system of congruences with $i \neq j$,

$$\begin{cases} x \equiv a_i \pmod{m_i} \\ x \equiv a_j \pmod{m_j} \end{cases}$$

has a solution, say x_0. Then $x_0 - a_i = c_i m_i$ with some integer c_1. Substituting this into the second congruence, we get $a_1 + c_1 m_1 - a_j = c_2 m_2$ for some integer c_2.

Then

$$a_1 - a_2 = -c_1 m_1 + c_2 m_2 = r(m_1, m_2)$$

for some integer r . Thus $a_1 - a_2$ is congruent to the greatest common divisor of m_i and m_j .

Now we proceed the uniqueness of the solution of the system of congruences (0.1) $\mod[m_1, m_2, \cdots, m_k]$. Suppose that x and y are solutions of the system (0.1). Repeating exactly the same argument as in the proof of the ordinary chinese remainder theorem, we have, for $i = 1, 2, \cdots, k$,

$$x - y \equiv 0 \pmod{m_i} .$$

Then obviously

$$x \equiv y \pmod{[m_1, m_2, \cdots, m_k]} .$$

Finally we prove the sufficiency. Here we put $M = [m_1, m_2, \cdots, m_k]$ the least common multiple of m_i's . Then we can express M in the form

$$M = \prod_{i=1}^{k} \mu_i , \tag{3.1}$$

of relatively prime factors, including unity, such that μ_i divides m_i for $i = 1, 2, \cdots, k$. Then we can find y_i satisfying, for $i = 1, 2, \cdots, k$,

$$y_i \equiv 1 \pmod{\mu_i}$$

and

$$y_i \equiv 0 \pmod{M/\mu_j}$$

for all $j \neq i$. Now the number

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

is a solution of the system (0.1).

<Q. E. D.>

By using the expression (3.1) and tracing the argument in the proof of Theorem 1, we get the following:

Theorem 2. *Under the same assumptions as in the generalized chinese remainder theorem, the system of congruences* (0.1) *is equivalent to the following single linear congruence*

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

where b_i's *are arbitrary integers coprime to* μ_i's , *respectively, and* $M_i = M/\mu_i$, *for* $i = 1, 2, \cdots, k$ *with* $M = \prod_{i=1}^{k} \mu_i = [m_1, m_2, \cdots, m_k]$.

Remark 3.1. The chinese remainder theorem can be proved in an arbitrary principal ideal ring instead of the ring of rational integers. Thus our Theorem 1 can be generalized in an arbitrary principal ideal ring, and especially in every ring of polynomials of coefficients in an arbitrary field.

Remarks 3.2. Theorem 1 provides a simple procedure for the construction of confounding plans in mixed factorials. The details of these two Remarks will be discussed elsewhere.

References

[1] Dickson, E., *History of the Theory of Numbers*, vol. II, Diophantine Analysis. Chelsea (1971).

[2] Knuth, D., *The Art of Computer Programming*, vol. 2, Seminumerical Algorithms. Addison-Wesley (1969).

[3] Rosen, K., *Elementary Number Theory and its Applications*. Addison-Wesley (1984).