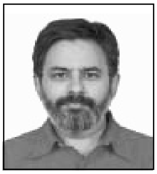
Multivariable Chinese Remainder Theorem

B Sury



B Sury was in the School of Mathematics of TIFR Bombay from 1981 to 1999. Since 1999, he has been with the Indian Statistical Institute in Bangalore. His research interests are in algebra and number theory. He is the Karnataka co-ordinator for the Mathematical Olympiad Programme in India.

Sun-Tsu wrote the treatise *Sunzi Suanjiing* around the 3rd century. The problem of finding an integer x which is simultaneously 2 modulo 3, 3 modulo 5 and 2 modulo 7 was considered. The smallest solution was found to be 23 and such a result is now called the Chinese Remainder Theorem (CRT). From early times – perhaps, from the 1st century itself – the CRT was employed in the preparation of calendars. In India, Aryabhata's mathematics from the 5th century contains instances of the CRT. However, a multivariable version of CRT does not seem to be well known and is not a part of textbooks. Qin Jiushao seems to have considered one such version in the 13th century. In this article, the basic CRT is recalled and some multivariable versions are studied using elementary linear algebra.

1. Introduction

The Chinese remainder theorem (CRT) seems to have originated in the work of Sun-Tsu in the 3rd century AD. There are also versions in Indian 5th century mathematics of Aryabhata. The classical versions dealt with coprime moduli. Oystein Ore proved a version [1] for non-coprime moduli in 1952 in the *American Mathematical Monthly*, but this does not seem to be well known because a paper published 50 years later by Howard [2] proves the same result! However, a multivariable version does not seem to be known. We present such a version and point out that there are still many questions open for investigation.

Keywords
Chinese remainder theorem, simultaneous congruences.

2. Classical CRT

A variant of a folklore tale goes as follows. Three thieves steal a number of gold coins and go to sleep after burying the loot. During the night, one thief wakes up and digs up the coins and, after distributing into 6 equal piles, finds 1 coin left over which he pockets quietly after burying the rest of the coins. He goes back to sleep and after a while another thief wakes up and digs up the coins. After making 5 equal piles, he again finds 1 coin left over which he pockets and buries the rest and goes to sleep. The 3rd thief wakes up and finds the rest of the coins make 7 equal piles excepting a coin which he pockets. If the total number of coins they stole is not more than 200, what is the exact number?

With a bit of hit and miss, one can find that 157 is a possible number. The Chinese remainder theorem gives a systematic way of solving this, in general.

In the above problem, the sought for natural number N is such that $(N-1)$ is a multiple of 6, $(N-2)$ is a multiple of 5 and $(N-3)$ is a multiple of 7. This means that N leaves *remainders* $1, 2, 3$ on division by $6, 5, 7$ respectively.

Let us consider two coprime natural numbers m_1 and m_2 and suppose, we are looking for a natural number N which leaves remainders a_1 and a_2 on division by m_1 and m_2, respectively. Then, the Euclidean division algorithm tells us that the smallest positive integer of the form $m_1k_1 + m_2k_2$ (for integers k_1 and k_2) is the greatest common divisor (GCD) of m_1 and m_2 (which is 1 in this case). Therefore, we have integers (of opposite signs) k_1 and k_2 such that

$$m_1k_1 + m_2k_2 = 1.$$

The number

$$N = a_1m_2k_2 + a_2m_1k_1$$

has the property that $(N - a_1)$ is a multiple of m_1 and $(N - a_2)$ is a multiple of m_2. We have not yet got a number as sought since N could be negative. However, we may add a suitable multiple of $m_1 m_2$ to N which will satisfy the requirements.

More generally, suppose there are r natural numbers $m_1, \cdots, m_r$ which are pairwise coprime. We seek a natural number N leaving given remainders $a_1, \cdots, a_r$ on divisions by $m_1, \cdots, m_r$ respectively. An appropriate generalization of the above argument for two numbers follows. If M_i denotes the product of all the m_j's excepting m_i, then the GCD of m_i and M_i is 1 for each $i = 1, \cdots, r$. As above, the Euclidean algorithm gives integers n_i, k_i such that

$$n_i M_i + k_i m_i = 1$$

for each $i = 1, \cdots, r$.

Therefore, $a_i n_i M_i - a_i$ is a multiple of m_i for each $i \leq r$.

As m_i divides M_j for each $j \neq i$, the integer,

$$N = a_1 n_1 M_1 + a_2 n_2 M_2 + \cdots + a_r n_r M_r\,,$$

is such that $(N - a_i)$ is a multiple of m_i for each $i \leq r$. Adding a suitable multiple of $m_1 m_2 \cdots m_r$, we can get a natural number N such that N leaves the remainder a_i on division by m_i, for each $i \leq r$.

Note that any other natural number N_0 satisfying the same property must differ from N by a multiple of each m_i and hence, of the product $m_1 m_2 \cdots m_r$.

In other words, there is a unique solution for N in the range $[1, m_1 m_2 \cdots m_r]$.

Here is a nice exercise.

If $m_1, \cdots, m_r$ are natural numbers which are not necessarily pairwise coprime, then there is a natural number

N yielding given remainders a_i on division by m_i if, and only if, the GCD of m_i and m_j divides $(a_i - a_j)$ for each i, j.

2.1 *Gauss and Congruences*

The great mathematician C F Gauss defined the algebraic notion of 'congruence' which generalizes the notion of equality of numbers and dramatically simplifies the proofs of several number-theoretic results. Given a natural number m, two integers x and y are said to be 'congruent modulo m' – written $x \equiv y \bmod m$ – if $(x-y)$ is an integral multiple of m.

Not surprisingly, the notation is also due to Gauss! Congruences to a fixed modulus behave much like equality. For instance, it is very easy to verify that:

$$x_1 \equiv y_1 \mod m \ , \ x_2 \equiv y_2 \mod m$$

implies

$$x_1 + x_2 \equiv y_1 + y_2 \bmod m, \quad x_1 x_2 \equiv y_1 y_2 \bmod m.$$

Further, we note that negative numbers are dealt on an equal footing; the statement that x leaves a remainder 3 on division by 4 can be written as $x \equiv -1 \bmod 4$. Note that if x leaves a remainder 3 on division by 4, then x^{2013} leaves the same remainder and, this is easier to see via congruences because

$$x \equiv -1 \bmod 4 \Rightarrow x^{2013} \equiv (-1)^{2013} = -1 \equiv 3 \bmod 4.$$

The argument that for two coprime integers m and n, $1 = mu + nv$ for integers u and v from the Euclidean division algorithm, can also be rephrased as asserting that 'Each of the two integers has a multiplicative inverse modulo the other'. That is, there exists an integer u (unique mod n – meaning unique up to adding multiples of n) such that $mu \equiv 1 \bmod n$ and, similarly, there is an integer v (unique mod m) such that $nv \equiv 1 \bmod m$.

The calculus of congruences is highly efficient in formulating and solving problems in elementary number theory.

We call u 'the multiplicative inverse of m mod n' keeping in mind that it is defined only up to addition of multiples of n.

The calculus of congruences is highly efficient in formulating and solving problems in elementary number theory. For instance, given a number with the digits $d_1 d_2 \cdots d_k$ in base 10, its remainder on division by 9 is simply that of the sum $\sum_{i=1}^{k} d_i$. Note that the given number could be as large as 10^{r-1} while the sum of its digits is at the most $9r$ which is much smaller for a large r; this reduces computation drastically.

In the language of congruences, the classical Chinese remainder theorem which we proved above can be recast as follows:

(Explicit) Chinese Remainder Theorem. *Let $m_1, \cdots, m_r$ be pairwise coprime natural numbers, and a_i $(1 \leq i \leq r)$ be arbitrary integers. Write $M_i = \prod_{j \neq i} m_j$. Let n_i be the multiplicative inverse of M_i modulo m_i. Then, the unique solution N mod $m_1 m_2 \cdots m_r$ to the system of congruences $N \equiv a_i$ mod m_i for all $i \leq r$ is given by*

$$N = a_1 n_1 M_1 + a_2 n_2 M_2 + \cdots + a_r n_r M_r.$$

3. Many-Variable CRT

Let us observe first that if c is an integer coprime to m and d is its multiplicative inverse modulo m, then $x = da$ is a solution to a congruence $cx \equiv a$ mod m. Therefore, the classical CRT can be formulated also as a system of congruences of the form $c_i x \equiv a_i$ mod m_i $(1 \leq i \leq r)$, where $(c_i, m_i) = 1$ for each i; the solution above changes to $N = \sum_{i=1}^{r} d_i a_i n_i M_i$, where $c_i d_i \equiv 1$ mod m_i. Thus, it is easy to formulate a multivariable version, where the left-hand sides are linear polynomials in several variables x_i's instead of a single one. However, we soon realize that a necessary and sufficient condition for the existence of a solution in general is far from obvious. We formulate and prove the following multivariable version and analyze later what else needs to be done.

Qin Jiushao is supposed to have come up with a multidimensional version of the CRT in the 13th century.

Theorem. *Let k and n be arbitrary positive integers and suppose a_{ij} are integers (for $1 \leq i \leq k, 1 \leq j \leq n$). Suppose $m_1, \cdots, m_k$ are pairwise coprime integers and $b_1, \cdots, b_r$ are arbitrary integers. Then, the k simultaneous congruences*

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{m_1},$$

$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 \pmod{m_2},$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n \equiv b_k \pmod{m_k}$$

have a solution in integers $x_1, \cdots, x_n$ if and only if, for each $i \leq k$, the GCD m_i of $a_{i1}, a_{i2}, \cdots, a_{in}$, divides b_i.

Proof. We apply induction on k to prove the theorem. The proof is constructive modulo the Euclidean division algorithm (which is also constructive).

Consider first the case $k = 1$.

If the integers $x_1, \cdots, x_n$ satisfy the congruence

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{m_1},$$

we have $\sum_{j=1}^{n} a_{1j}x_j - b_1 = m_1 t$ for some integer t. Thus, the greatest common divisor of $a_{11}, a_{12}, \cdots, a_{1n}$ and m_1 divides b_1. This condition is also sufficient by the Euclidean division algorithm. For, if $b_1 = sd$, where $d = \text{GCD}(a_{11}, \cdots, a_{1n}, m_1)$, then writing

$$d = \sum_{j=1}^{n} a_{1j}y_j + m_1 t,$$

we have a solution $x_1 = sy_1, \cdots, x_n = sy_n$ of the congruence

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{m_1}.$$

Therefore, for a general k, a necessary condition for a common solution is that, for each $i \leq k$, the GCD of $a_{i1}, a_{i2}, \cdots, a_{in}, m_i$ divides b_i.

This condition also ensures that each individual congruence has a solution.

Now, we suppose that the GCD conditions hold and that we have already arrived at a common solution $x_1, \cdots, x_n$ in integers for the first r congruences $(1 \leq r < k)$:

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \equiv b_i \pmod{m_i} \ \forall \ 1 \leq i \leq r.$$

Now, we first choose a solution $y_1, \cdots, y_n$ of the $(r+1)$-th congruence

$$a_{r+1,1}x_1 + a_{r+1,2}x_2 + \cdots + a_{r+1,n}x_n \equiv b_{r+1} \pmod{m_{r+1}}.$$

For each $j \leq n$, choose X_j such that

$$m_1m_2 \cdots m_r X_j \equiv y_j - x_j \pmod{m_{r+1}}.$$

These choices are possible because $m_1m_2 \cdots m_r$ and m_{r+1} are relatively prime. We observe that for the new choices,

$$x'_j = x_j + m_1m_2 \cdots m_r X_j \quad (1 \leq j \leq n),$$

the first r congruences continue to hold. Moreover,

$$\sum_{j=1}^{n} a_{r+1,j}x'_j \equiv \sum_{j=1}^{n} a_{r+1,j}(x_j + m_1m_2 \cdots m_r X_j)$$

$$\equiv \sum_{j=1}^{n} a_{r+1,j}y_j \equiv b_{r+1} \pmod{m_{r+1}}.$$

Therefore, the theorem is proved by induction.

4. Remarks

(i) The classical Chinese remainder theorem can be thought of as the special case when the matrix $\{a_{ij}\}$ has only a single column which is non-zero.

(ii) If the matrix $\{a_{ij}\}$ has a left inverse (that is an $n \times k$ integer matrix $\{b_{ij}\}$ such that $BA = I_n$), then clearly the necessary condition of the theorem holds for any choice of $b_1, \cdots, b_k$.

In particular, if $k = n$ and $\{a_{ij}\}$ is an $n \times n$ integral matrix whose inverse is also integral, each system of n linear congruences in n variables with pairwise coprime moduli has a solution.

(iii) A special case of the above theorem, which is of interest as it produces a solution for arbitrary b_i's, is the following one. In the theorem above, if, for each $i \leq k$, there is some j for which a_{ij} is coprime to m_i, then the necessary condition obviously holds.

(iv) In the classical case of one variable, there is a unique solution modulo $m_1 m_2 \cdots m_k$. In the multivariable case, there is no natural uniqueness assertion possible. The point is that homogeneous congruences in more than one variable have many solutions. So, uniqueness can be asked for only after specifying a box (in n dimensions, with volume $m_1 m_2 ....m_k$) in which we seek solutions.

For example, both $(1, 4)$ and $(0, -1)$ are simultaneous solutions of the congruences

$$x - y \equiv 1 \pmod{2},$$

$$x + y \equiv 2 \pmod{3}.$$

(v) The Euclidean division algorithm is the principal reason behind these classical versions of the Chinese remainder theorem. In particular, it holds good over the polynomial ring in one variable over a field. If n elements are coprime, then there is a linear combination which gives 1. This is no longer true if we consider, for instance, polynomials in two variables.

X and *Y* are polynomials without common factors but there do not exist polynomials *f*,*g* in *X* and *Y* such that *X f*(*X*,*Y*) + *Y g*(*X*,*Y*) = 1.

For example, in the polynomial ring $C[X, Y]$, consider the congruences

$$t \equiv 0 \pmod{X},$$

$$t \equiv 1 \pmod{Y}.$$

Here, of course, by a congruence $f(X, Y) \equiv g(X, Y) \bmod h(X, Y)$, we mean that there is a polynomial $k(X, Y)$ so that

$$h(X, Y)k(X, Y) = f(X, Y) - g(X, Y).$$

There is no common solution of the two congruences mentioned above as there do not exist polynomials f, g for which $Xf + Yg = 1$.

(vi) The Chinese remainder theorem has been generalized to rings and modules. But, none of the versions is an analogue of the many-variable cases proved above.

5. General Moduli for Multivariable CRT

Here, we point out a criterion which is sufficient to ensure the existence of a solution when the moduli m_i's are general (that is, not necessarily pairwise coprime).

The case of general moduli is equivalent to a system of congruences for prime power moduli. By the above theorem, we need to look at only the case when all the moduli are powers of a single prime p. If we can get a necessary and sufficient criterion for these cases, we will get such a criterion for the general case. In this section, we fix a prime p and moduli $m_i = p^{t_i}$. We further consider only the special case of n congruences in n variables. That is, let us look at an $n \times n$ integer matrix $A = \{a_{ij}\}$ and at the corresponding system of congruences

$$\sum_{j=1}^{n} a_{ij}x_j \equiv b_i \pmod{p^{t_i}} \;\; \forall \;\; i \leq n.$$

We write $b_i = p^{\beta_i}u'_i$ and $\det(A) = p^{\delta}d$, where u'_i, d are not divisible by p. A sufficient criterion is the following one:

Lemma. *If $\delta \leq \beta_i \leq t_i$ for all $i \leq n$, then the simultaneous system of congruences above has a common solution.*

Proof. The proof is straightforward.

Write the system of congruences as an equality $Ax = b + mu$ for some $u_1, \cdots, u_n$, where we have written x, b, m as columns and where x and u need to be shown to exist. Here, m is the column $(p^{t_1}, p^{t_2}, \cdots, p^{t_n})^t$.

If $B = adj(A)$ is the adjoint matrix of A, then multiplying the matrix equation on the left by $B = \{b_{ij}\}$, we have $\det(A)x = B(b + mu)$, i.e.,

$$p^\delta dx_i = \sum_{j=1}^{n} b_{ij}(p^{\beta_j}u'_j + p^{t_j}u_j) \ \forall\ i \leq n.$$

By the hypothesis, all the terms in the equality below are integers.

$$\begin{aligned} dx_i &= \sum_{j=1}^{n} b_{ij}(p^{\beta_j-\delta}u'_j + p^{t_j-\delta}u_j) \\ &= \sum_{j=1}^{n} b_{ij}p^{\beta_j-\delta}(u'_j + p^{t_j-\beta_j}u_j) \ \ \forall \ \ i \leq n. \end{aligned}$$

As $(p, d) = 1$, we may choose u_j's satisfying

$$p^{t_j-\beta_j}u_j \equiv -u'_j \pmod{d} \ \ \forall \ \ j.$$

Write $u'_j + p^{t_j-\beta_j}u_j = dy_j$ for $j \leq n$; then, we have

$$x_i = \sum_{j=1}^{n} b_{ij}p^{\beta_j-\delta}y_j \ \ \forall \ \ i \leq n.$$

Hence, we have a simultaneous solution to the congruences.

6. A Question for Investigation

Although sufficient conditions such as the one above can be formulated, it is not clear (unlike the single variable case) how to formulate a general necessary and sufficient condition for the multivariable Chinese remainder theorem when the moduli are not necessarily pairwise coprime.

Address for Correspondence
B Sury
Stat-Math Unit
Indian Statistical Institute
8th Mile Road
Bangalore 560 059, India.
Email: sury@isibang.ac.in

Suggested Reading

[1] Oystein Ore, The general Chinese remainder theorem, *The American Mathematical Monthly*, Vol.59, No.6, pp.365–370, 1952.

[2] Fredric T Howard, A generalized Chinese remainder theorem, *The College Mathematics Journal*, Vol.33, No.4, pp.279–282, September, 2002.