Chapter 2

Remodulization of Congruences

Proceedings—NCUR VI. (1992), Vol. II, pp. 1036–1041.

Jeffrey F. Gold

Department of Mathematics, Department of Physics
University of Utah

Don H. Tucker

Department of Mathematics
University of Utah

Introduction

Remodulization introduces a new method applied to congruences and systems of congruences. We prove the Chinese Remainder Theorem using the remodulization method and establish an efficient method to solve linear congruences. The following is an excerpt of *Remodulization of Congruences and its Applications* [2].

Definition 1 *If a and b are integers, then* $a \bmod b = \{a, a \pm b, a \pm 2b, \dots\}$.

We write $x \equiv a \ mod \ b$, meaning that x is an element of the set $a \ mod \ b$. The common terminology is to say that x is congruent to a *modulo* b. These sets are frequently called residue classes since they consist of those numbers which, upon division by b, leave a remainder (residue) of a.

Definition 2 *If $a_1, a_2, \ldots, a_n, b$ are integers, then*

$$[a_1, a_2, \ldots, a_n] \bmod b = (a_1 \bmod b) \cup (a_2 \bmod b) \cup \cdots \cup (a_n \bmod b) \ .$$

Theorem 1 *Suppose a, b, and c are integers and $c > 0$, then*

$$a \bmod b = [a, a+b, \ldots, a+(c-1)b] \bmod cb \ .$$

Proof. We write

$$\begin{array}{rcl} a \bmod b & = & \{ \begin{array}{llll} a-2cb, & a-(2c-1)b, & \ldots & a-(c+1)b \\ a-cb, & a-(c-1)b, & \ldots & a-b \\ a, & a+b, & \ldots & a+(c-1)b, \\ a+cb, & a+(c+1)b, & \ldots & a+(2c-1)b, \\ a+2cb, & a+(2c+1)b, & \ldots & a+(3c-1)b, \quad \} \end{array} \end{array}$$

and rewriting the rows

$$\begin{array}{rcl} a \bmod b & = & \{ \begin{array}{llll} a-2cb, & a+b-2cb, & \ldots & a+(c-1)b-2cb \\ a-cb, & a+b-cb, & \ldots & a+(c-1)b-cb \\ a, & a+b, & \ldots & a+(c-1)b, \\ a+cb, & a+b+cb, & \ldots & a+(c-1)b+cb, \\ a+2cb, & a+b+2cb, & \ldots & a+(c-1)b+2cb, \quad \} \end{array} \end{array}$$

Then, forming unions on the *extended* columns, the result follows. We refer to this process as remodulization by a factor c.

Suppose it is desired to express 1 *mod* 2 in terms of *modulo* 8, then, 1 *mod* 2 is remodulized by the factor 4, i.e.,

$$1 \bmod 2 = [1, 3, 5, 7] \bmod 8 \ .$$

It is convenient to create a notation for the expression

$$[\ a, a+b, \ldots, a+(c-1)b] \bmod cb \ .$$

We write it as

$$\bigcup_{k=0}^{c-1} [a+kb] \bmod cb \ .$$

Reindexing the symbol $\bigcup$,

$$a \bmod b = \bigcup_{k=1}^{c} [(a-b)+kb] \bmod cb \ .$$

The Chinese Remainder Theorem first appeared in the first century A.D. The Chinese mathematician Sun-Tsŭ sought a solution to the following problem:

What numbers n, when divided by 3, 5, and 7, have remainders 2, 3, and 2, respectively?

This problem also appeared in the *Introductio Arithmeticae*, written by Nicomachus of Gerasa, a Greek mathematician circa 100 A.D.

The problem asks one to find the solution to a system of congruences

$$(\dagger) \quad \begin{cases} x & \equiv & a_1 \bmod b_1 \\ x & \equiv & a_2 \bmod b_2 \\ & \vdots & \\ x & \equiv & a_n \bmod b_n \end{cases}$$

where $0 \leq a_j < b_j$, and the b_j are pairwise relatively prime.

The idea is to remodulize each congruence in order to obtain a common modulus, thereby making the solution set the intersection of the resulting classes. These can be determined by direct observation of the sets of residues in the remodulized forms.

Since the b_j are pairwise relatively prime, the smallest common modulus is the product of the b_j; therefore we remodulize the j^{th} congruence by the factor

$$\frac{1}{b_j}\prod_{k=1}^{n} b_k = c_j \ ; \quad then \ \ b_j c_j = C = \prod_{k=1}^{n} b_k$$

Performing these operations gives:

$$x_j \ \equiv \ \bigcup_{m=1}^{\frac{1}{b_j}\prod_{k=1}^{n} b_k} [(a_j - b_j) + b_j m] \bmod \prod_{k=1}^{n} b_k$$

Simplifying the notation, we find

$$x_j \equiv \bigcup_{m=1}^{c_j} [(a_j - b_j) + b_j m] \bmod C \ .$$

The solution set to (†) is the intersection of the sets of initial elements mod C, i.e.,

$$(\ddagger) \quad x \equiv \bigcap_{j=1}^{n} \left[\bigcup_{m=1}^{c_j} [(a_j - b_j) + b_j m] \bmod C \right].$$

Thus, for the original problem of Sun-Tsŭ, we have:

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

Since the b_j are prime, the least common modulus is $3 \cdot 5 \cdot 7 = 105$. The congruences are then remodulized by 35, 21, and 15, respectively. The resulting remodulizations are

[2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, 71, 74, 77, 80, 83, 86, 89, 92, 95, 98, 101, 104] mod 105 ;

[3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58, 63, 68, 73, 78, 83, 88, 93, 98, 103] mod 105 ; and

[2, 9, 16, 23, 30, 37, 44, 51, 58, 65, 72, 79, 86, 93, 100] mod 105 ,

where the intersection, 23 *mod* 105, is the complete solution set among the integers.

This ultimately raises the question as to whether

$$(\ddagger) \qquad x \equiv \bigcap_{j=1}^{n} \left[\bigcup_{m=1}^{c_j} [(a_j - b_j) + b_j m] \bmod C \right]$$

always contains *exactly* one element, given that $0 \leq a_j < b_j$ and the b_j are pairwise relatively prime.

In the same example, if we remodulize to the product 105, we find that the solution set corresponding to the first two congruences

$$\begin{cases} x & \equiv & 2 \bmod 3 \\ x & \equiv & 3 \bmod 5 \end{cases}$$

is characterized as $[8, 23, 38, 53, 68, 83, 98]$ *mod* 105, which does not appear to be "unique"; however, this is equivalent to 8 *mod* 15, which, in the example given, has been remodulized by the factor 7. The solution 8 *mod* 15 is obtained by solving the first two congruences directly by the method described. As it happens, if one uses the smallest possible modulus, the answer to our question is yes.

Theorem 2 (*ChineseRemainderTheorem*) *The system* (†) *of congruences, where the* b_j *are pairwise relatively prime, has as solution set*

$$(\ddagger) \qquad x \equiv \bigcap_{j=1}^{n} \left[\bigcup_{m=1}^{c_j} [(a_j - b_j) + b_j m] \bmod C \right]$$

where $c_j = \frac{C}{b_j}$ *and* $C = \prod_{k=1}^{n} b_k$. *Moreover, the intersection contains only one element, i.e., one residue class.*

Proof. In order to show that this element exists, we consider the following:

$$\begin{cases} x & \equiv & a_1 \bmod b_1 \\ x & \equiv & a_2 \bmod b_2 \end{cases}$$

where $0 \leq a_1 < b_1$ and $0 \leq a_2 < b_2$ and $gcd(b_1, b_2) = 1$. Remodulizing the congruences by the factors b_2 and b_1, respectively,

$$\begin{array}{rcl} x & \equiv & [a_1, a_1 + b_1, \ldots, a_1 + (b_2 - 1)\ b_1\ ] \bmod b_1 b_2 \\ x & \equiv & [a_2, a_2 + b_2, \ldots, a_2 + (b_1 - 1)\ b_2\ ] \bmod b_1 b_2 \end{array}$$

it is required to show that the sets of initial elements intersect, i.e., there exist integers k and h where $1 \leq k \leq b_2 - 1$ and $1 \leq h \leq b_1 - 1$, such that $a_1 + kb_1 = a_2 + hb_2$. Rewriting this equation, we require integers k and h such that $kb_1 - hb_2 = a_2 - a_1$.

Since b_1 and b_2 are relatively prime, $(a_2 - a_1)$ is divisible by $gcd(b_1, b_2)$. Now notice that if k and h are solutions to $kb_1 - hb_2 = 1$, then $k(a_2 - a_1)$ and $h(a_2 - a_1)$ are solutions to the required equation. Euclid's algorithm insures that such integers k and h exist.

It follows that the first pair of congruences have a solution. We wish now to show that the pair has a unique solution *modulo* $b_1 b_2$. We know that a solution exists, that is, there exists an integer x such that

$$x \in \{a_1, a_1 + b_1, \ldots, a_1 + (b_2 - 1)b_1\} \cap \{a_2, a_2 + b_2, \ldots, a_2 + (b_1 - 1)b_2\}.$$

Now suppose that the two initial sets intersect in two elements, say

$$x_1 = a_1 + \lambda b_1 = a_2 + kb_2$$

and

$$x_2 = a_1 + \mu b_1 = a_2 + hb_2\ .$$

Subtracting the second formulation from the first for each x_i,

$$a_1 - a_2 = kb_2 - \lambda b_1 = hb_2 - \mu b_1\ ,$$

so that

$$(k - h)b_2 = (\lambda - \mu)b_1\ .$$

Since b_1 and b_2 are relatively prime it must be that

$$k - h = mb_1 \quad and \quad \lambda - \mu = nb_2\ ,$$

for some integers m and n. In other words,

$$k = h + mb_1 \quad and \quad \lambda = \mu + nb_2$$

so that x_1 becomes

$$\begin{aligned} x_1 &= a_1 + (\mu + nb_2)b_1 &= a_2 + (h + mb_1)b_2 \\ &= a_1 + \mu b_1 + nb_2b_1 &= a_2 + hb_2 + mb_1b_2 \ . \end{aligned}$$

This says that

$$a_1 + \mu b_1 = a_2 + hb_2 + (m - n)b_1b_2 \ ,$$

which is x_2. This implies that $m - n = 0$; i.e., $m = n$, and hence

$$\begin{aligned} k &= h + mb_1 \\ \lambda &= \mu + mb_2 \ . \end{aligned}$$

Therefore,

$$\begin{aligned} x_1 &= a_1 + \lambda b_1 = a_1 + (\mu + mb_2)b_1 \\ &= a_1 + \mu b_1 + mb_1b_2 \\ &= x_2 + mb_1b_2 \ . \end{aligned}$$

This means that x_1 and x_2 are in the same residue class *mod* b_1b_2; i.e., they are congruent *mod* b_1b_2 and the solution set is given as the unique class

$$x \equiv d \bmod b_1b_2 \ ,$$

where $d \equiv x_1 \bmod b_1b_2 \equiv x_2 \bmod b_1b_2$ from above.

In the event there exist *three* congruences, we solve the first two congruences and combine this result with the third congruence, i.e.,

$$\begin{cases} x \equiv d \bmod b_1b_2 \\ x \equiv a_3 \bmod b_3 \end{cases}$$

and repeat the argument since b_1b_2 and b_3 are relatively prime. The induction works and both the existence and the uniqueness are established.

Suppose we want to solve $cx \equiv a \ mod \ b$ for x, where $1 < c < b$ and a is divisible by $gcd(c, b)$ (otherwise no solution exists). We consider the case where $gcd(c, b) = 1$. By remodulizing $a \ mod \ b$ by the factor c, we obtain

$$cx \equiv [a, a + b, \ldots , a + (c - 1)\ b\ ] \bmod cb.$$

Since the set $\{a, a+b, \ldots , a+(c-1)\ b\}$ forms a complete residue system *mod* c, there exists an element in this set, call it d, which is divisible by c. Since

$$cx \equiv [a, a + b, \ldots , d, \ldots , a + (c - 1)b] \bmod cb$$

we find that the only congruence solvable is $cx \equiv d \ mod \ cb$. The remaining congruences,

$$cx \equiv [a, a + b, \ldots , d - b, d + b, \ldots , a + (c - 1)\ b\ ] \bmod cb$$

are not solvable, since in each case the factor c is pairwise relatively prime with the elements $\{a, a+b, \ldots, d-b, d+b, \ldots, a+(c-1)b\}$, and thus does not divide them. In the congruence $cx \equiv d \ mod \ cb$, dividing through by c,

$$x \equiv \frac{d}{c} \bmod \frac{cb}{c} \quad or \quad x \equiv \frac{d}{c} \bmod b \ .$$

Note that $\frac{d}{c} < b$.

To illustrate this procedure, consider the following example. Suppose $5x \equiv 3 \ mod \ 7$. This is solvable since 3 is divisible by $gcd(5,7) = 1$. Remodulizing $3 \ mod \ 7$ by the factor 5 gives

$$5x \equiv [3, 10, 17, 24, 31] \bmod 5 \cdot 7$$

so that $5x \equiv 10 \ mod \ 35$ is the only possible solution and, upon dividing all three terms by 5,

$$x \equiv 2 \bmod 7 \ .$$

Note that $5x \equiv [3, 17, 24, 31] \bmod 35$ does not yield any solutions, since in this case $gcd(5, 35) = 5$ does not divide any number in the set $\{3, 17, 24, 31\}$.

The remodulization method also provides a way of finding solutions to systems of congruences using linear congruences. Suppose we have the following system,

$$\begin{cases} x & \equiv & a_1 \bmod b_1 \\ x & \equiv & a_2 \bmod b_2 \end{cases}$$

where $b_1 < b_2$ and b_1 and b_2 are relatively prime. The idea is to multiply the first congruence by b_2 and the second congruence by b_1, i.e.,

$$\begin{cases} b_2 x & \equiv & a_1 b_2 \bmod b_1 b_2 \\ b_1 x & \equiv & a_2 b_1 \bmod b_1 b_2 \end{cases}$$

so that we obtain a common modulus. By subtracting the second linear congruence from the first, we obtain a single linear congruence,

$$(b_2 - b_1)x \equiv (a_1 b_2 - a_2 b_1) \bmod b_1 b_2 \ .$$

The unique solution ($modulo \ b_1 b_2$) is insured, since $gcd(b_2 - b_1, b_1 b_2) = 1$. If the system consists of more than two congruences, then the solution of the first two congruences is combined with the third, and so on, to obtain a solution for the entire system.

Corollary 1 *A system of linear congruences*

$$\begin{cases} c_1 x & \equiv & a_1 \bmod b_1 \\ c_2 x & \equiv & a_2 \bmod b_2 \\ & \vdots & \\ c_n x & \equiv & a_n \bmod b_n \end{cases}$$

where $1 < c_j < b_j$, the b_j are pairwise relatively prime, and the a_j are divisible by $gcd(c_j, b_j)$, can be reduced to a system

$$\begin{cases} x & \equiv & d_1 \bmod b_1 \\ x & \equiv & d_2 \bmod b_2 \\ & \vdots & \\ x & \equiv & d_n \bmod b_n \ . \end{cases}$$

By Theorem 2, the solution to this system is

$$x \equiv \bigcap_{j=1}^{n} \left[\bigcup_{m=1}^{c_j} [(d_j - b_j) + b_j m] \bmod C \right]$$

where $c_j = \frac{1}{b_j} \prod_{k=1}^{n} b_k$ and $C = \prod_{k=1}^{n} b_k$, and the intersection contains only one residue class.

References

[1] Burton, David M. *Elementary Number Theory, Second Edition.* Wm. C. Brown Publishers, Dubuque, Iowa, 1989.

[2] Gold, J. F. and Don H. Tucker. *Remodulization of Congruences and Its Applications.* To be submitted.

[3] Ore, Oystein. *Number Theory and Its History.* Dover Publications, Inc., New York, 1988.

[4] Stewart, B. M. *Theory of Numbers.* The MacMillan Co., New York, 1952.