Chapter 4

Complementary Sets Of Systems Of Congruences

Proceedings—NCUR VII. (1993), Vol. II, pp. 793–796.

Jeffrey F. Gold

Department of Mathematics, Department of Physics
University of Utah

Don H. Tucker

Department of Mathematics
University of Utah

Introduction

We introduce remodulization and use it to characterize the complementary sets of systems of congruences. The following is an excerpt of a continuing effort to characterize systems of congruences.

Remodulization

Definition 1 *If a and b are integers, then*

$$a \bmod b = \{a, a \pm b, a \pm 2b, \ldots\} .$$

We will write $x \equiv a \ mod \ b$, meaning that x is an element of the set $a \ mod \ b$. (The symbol $\equiv$ is not an equality symbol, but rather a specialized form of the "$\in$" or "is an element of ..." symbol). The common terminology is to say that x

is congruent to a *modulo* b. These sets are also frequently called residue classes since they consist of those integers which, upon division by b, leave a remainder (residue) of a. It is customary to write a as the least non-negative residue.

Definition 2 *If* $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$, *then*

$$[a_1, a_2, \ldots, a_n] \bmod b = (a_1 \bmod b) \cup (a_2 \bmod b) \cup \cdots \cup (a_n \bmod b) = \bigcup_{i=1}^{n} a_i \bmod b \, .$$

Theorem 1 *(Remodulization Theorem) Suppose* a, b, *and* $c \in \mathbb{Z}$ *and* $c > 0$, *then*

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

Proof. We write

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

and upon rewriting the columns,

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

Then, forming unions on the *extended* columns, the result follows.

We refer to this process as remodulization by a factor c.

Complementary Sets

Using Definition 2, the complementary set of a *mod* b is given by

$$[a \bmod b]^c = \mathbb{Z} \setminus \{a \bmod b\} = [0, 1, 2, \ldots, a-1, a+1, \ldots, b-1] \bmod b \, .$$

In this case, the complementary set consists of $b-1$ congruences *modulo* b. We will always refer to the size of a complementary set with respect to a specific modulus.

The following represents a system of congruences:

$$\left\{ \begin{array}{rcl} x & \equiv & a_1 \bmod b_1 \\ x & \equiv & a_2 \bmod b_2 \\ & \vdots & \\ x & \equiv & a_n \bmod b_n \end{array} \right. \tag{4.1}$$

Characterizing the size of the complementary set of a system of congruences (4.1) is equivalent to counting those integers which are not elements of any of the given congruences. Our method will be to remove the set of numbers satisfying the system of congruences (4.1) from the set of integers $\mathbb{Z}$ in a systematic way. Note that $\mathbb{Z}$ can be written as a complete residue class, $[1, 2, \ldots, b]$ *mod* b, for all $b > 1$.

All numbers satisfying the first congruence in (4.1) will be removed from $\mathbb{Z}$, leaving the complementary set for that congruence. Then we iterate the process by removing all integers satisfying the second congruence from this remaining set, and so on.

Stated another way, we are interested in determining the size of

$$[a_1 \bmod b_1 \cup a_2 \bmod b_2 \cup \cdots \cup a_n \bmod b_n]^c \;=\; \mathbb{Z} \setminus \left\{ \bigcup_{i=1}^{n} a_i \bmod b_i \right\} \;,$$

where the b_i are pairwise relatively prime. Our method is to determine the number of (remaining) congruences needed to characterize this complementary set. Using the remodulization method, the set of congruences can be expressed in terms of the common modulus, *mod* $\prod_{i=1}^{n} b_i$ and the integers, $\mathbb{Z}$, can be expressed in terms of a complete residue class of the *same* modulus.

To illustrate this procedure, suppose we have the following system of congruences

$$\left\{ \begin{array}{lcl} x & \equiv & a_1 \bmod b_1 \\ x & \equiv & a_2 \bmod b_2 \end{array} \right.$$

where $gcd(b_1, b_2) = 1$. By the **Chinese Remainder Theorem** [1,2], these intersect in a unique residue class *modulo* $b_1 b_2$.

Remodulizing the congruences by b_2 and b_1, respectively, this system can be expressed as

$$\left\{ \begin{array}{lcl} a_1 \bmod b_1 & = & [a_1, a_1 + b_1, \ldots, a_1 + b_1(b_2 - 1)] \bmod b_1 b_2 \\ a_2 \bmod b_2 & = & [a_2, a_2 + b_2, \ldots, a_2 + b_2(b_1 - 1)] \bmod b_1 b_2 \end{array} \right.$$

The first congruence, after remodulization, consists of b_2 congruences *mod* $b_1 b_2$ while the second remodulized congruence consists of b_1 congruences *mod* $b_1 b_2$; furthermore, $\mathbb{Z}$ consists of $b_1 b_2$ congruences (*modulo* $b_1 b_2$). Therefore, subtracting b_1 and b_2 from $b_1 b_2$ and adding one to this sum (the unique intersection of the two congruences was removed twice from $b_1 b_2$), we obtain

$$b_1 b_2 - b_1 - b_2 + 1$$

remaining congruences *mod* $b_1 b_2$ in the complementary set

$$[a_1 \bmod b_1 \cup a_2 \bmod b_2]^c \;.$$

However, $b_1b_2 - b_1 - b_2 + 1$ can be rewritten as $(b_1 - 1)(b_2 - 1)$; this is typical.

Theorem 2 *The complementary set of* $\{\bigcup_{i=1}^{n} a_i \bmod b_i\}$, *where the* b_i *are pairwise relatively prime, contains exactly* $\prod_{i=1}^{n}(b_i - 1)$ *congruences modulo* $\prod_{i=1}^{n} b_i$.

Proof. Suppose we have a system of congruences (4.1) where the b_i are pairwise relatively prime. We have already found that the complementary sets of a_1 *mod* b_1 and a_1 *mod* $b_1 \cup a_2$ *mod* b_2 consist of $(b_1 - 1)$ congruences *modulo* b_1 and $(b_2 - 1)(b_1 - 1)$ congruences *modulo* b_1b_2, respectively.

For the induction argument, suppose we have found the complementary set up to k^{th} congruence of (4.1) to consist of the union of $\prod_{i=1}^{k}(b_i - 1)$ congruences *modulo* $\prod_{i=1}^{k} b_i$; then we remove from it the set of numbers congruent $\{a_{k+1}$ *mod* $b_{k+1}\}$. The complementary set of the latter congruence is comprised of $(b_{k+1} - 1)$ congruences *modulo* b_{k+1}. Each of these congruences shares a unique intersection with each of the congruences in the remaining complementary set; there are $(b_{k+1} - 1)\prod_{i=1}^{k}(b_i - 1)$ such intersections *modulo* $\prod_{i=1}^{k+1} b_i$. Therefore, the remaining complementary set, after removing the $(k+1)^{st}$ congruence from the remaining complementary set, consists of

$$\prod_{i=1}^{k+1}(b_i - 1)$$

congruences *modulo* $\displaystyle\prod_{i=1}^{k+1} b_i$.

If the moduli b_i are primes, then we may use Euler's phi function [3,4], or totient, to formulate the complementary set of a system of congruences. The totient $\Phi(m)$ counts the number of integers not exceeding m which are relatively prime to m. For any prime p, $\Phi(p) = p - 1$; moreover, because the totient is multiplicative, $\Phi(p_1p_2 \cdots p_n) = \Phi(p_1)\Phi(p_2) \cdots \Phi(p_n) = \prod_{i=1}^{n}(p_i - 1)$.

Corollary 1 *Suppose we have a system of congruences where the moduli* p_i *are primes and* $p_i \neq p_j$, *for* $i \neq j$. *Then the complementary set of*

$$\begin{cases} x & \equiv & a_1 \bmod p_1 \\ x & \equiv & a_2 \bmod p_2 \\ & \vdots & \\ x & \equiv & a_n \bmod p_n \end{cases}$$

consists of $\Phi\left(\displaystyle\prod_{i=1}^{n} p_i\right)$ *congruences modulo* $\displaystyle\prod_{i=1}^{n} p_i$.

Definition 3 *The density of the complementary set of a system of congruences (4.1), where* $gcd(b_i, b_j) = 1$ *for* $i \neq j$*, with respect to the set* $\mathbb{Z}$*, is*

$$\rho(n) = \prod_{i=1}^{n} \left(\frac{b_i - 1}{b_i} \right) \ .$$

As an illustration, we calculate the size and density of the complementary set of the following system:

$$\begin{cases} x & \equiv & 1 \bmod 3 \\ x & \equiv & 2 \bmod 5 \\ x & \equiv & 3 \bmod 7 \end{cases}$$

The complement of the first congruence, 1 *mod* 3, is $[2, 3]$ *mod* 3, a union of two congruences *modulo* 3. The complement of 2 *mod* 5 is $[1, 3, 4, 5]$ *mod* 5. Each of the congruences in the complementary set *modulo* 3 shares a unique intersection with the congruences of the complementary set *modulo* 5; there are $(3-1)(5-1) = 8$ remaining congruences *modulo* 15. Finally, removing all numbers satisfying 3 *mod* 7 from these 8 remaining congruences, the complementary set consists of $(3-1)(5-1)(7-1) = 48$ congruences *modulo* 105. The density of the complementary set with respect to the set $\mathbb{Z}$ at each step in the process is 2/3, 8/15, and 48/105, respectively.

If a system consists of α_{b_i} congruences of the *same* modulus b_i, for each b_i, we have the following extension of Theorem 2. Suppose

$$\begin{cases} x & \equiv & [a_{1,1}, a_{1,2}, \ldots, a_{1,\alpha_{b_1}}] \bmod b_1 \\ x & \equiv & [a_{2,1}, a_{2,2}, \ldots, a_{2,\alpha_{b_2}}] \bmod b_2 \\ & \vdots & \\ x & \equiv & [a_{n,1}, a_{n,2}, \ldots, a_{n,\alpha_{b_n}}] \bmod b_n \end{cases} \tag{4.2}$$

where the b_i are pairwise relatively prime, and $a_{i,j} \neq a_{i,k}$ for all $j \neq k$, and $\alpha_{b_i} < b_i$.

The complementary set of the first congruence is the union of $b_1 - \alpha_{b_1}$ congruences. Likewise, the complementary set of the second congruence contains $b_2 - \alpha_{b_2}$ congruences; their intersection contains $(b_2 - \alpha_{b_2})(b_1 - \alpha_{b_1})$ congruences *modulo* $b_1 b_2$. Iterating the process, the complementary set of (4.2) consists of $\prod_{i=1}^{n}(b_i - \alpha_{b_i})$ congruences *modulo* $\prod_{i=1}^{n} b_i$. At each step, however, it is necessary to insure that $b_i - \alpha_{b_i} > 0$; otherwise, if $\alpha_{b_i} = b_i$, the complementary set vanishes altogether, since for that particular value of i, $[a_{i,1}, a_{i,2}, \ldots, a_{i,\alpha_{b_i}}]$ is a complete residue class *modulo* b_i, i.e., the entire set $\mathbb{Z}$.

Theorem 3 *The complementary set of* $\left\{ \bigcup_{i=1}^{n} [a_{i,1}, \ldots, a_{i,\alpha_{b_i}}] \bmod b_i \right\}$*, where* $a_{i,j} \neq a_{i,k}$ *for* $j \neq k$*, and* $\alpha_{b_i} < b_i$*, and the* b_i *are pairwise relatively prime,*

contains exactly $\prod_{i=1}^{n}(b_i - \alpha_{b_i})$ *congruences modulo* $\prod_{i=1}^{n} b_i$. *The density of the complementary set is* $\rho(n) = \prod_{i=1}^{n}\left(\frac{b_i - \alpha_{b_i}}{b_i}\right)$.

References

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

[2] Gold, Jeffrey F. and Don H. Tucker, *Remodulization of Congruences*, Proceedings - National Conference on Undergraduate Research, (University of North Carolina Press, Asheville, North Carolina, 1992), Vol. II, pp. 1036–41.

[3] David M. Burton, *Elementary Number Theory* (Wm. C. Brown Publishers, Iowa, 1989), Second Edition, pp. 156–160.

[4] Oystein Ore, *Number Theory and Its History* (Dover Publications, Inc., New York, 1988), pp. 109–115.