Chapter 6

A Novel Solution Of Linear Congruences

Proceedings—NCUR IX. (1995), Vol. II, pp. 708–712

Jeffrey F. Gold

Department of Mathematics, Department of Physics
University of Utah
Salt Lake City, Utah 84112

Don H. Tucker

Department of Mathematics
University of Utah
Salt Lake City, Utah 84112

Introduction

Although the solutions of linear congruences have been of interest for a very long time, they still remain somewhat pedagogically difficult. Because of the importance of linear congruences in fields such as public-key cryptosystems, new and innovative approaches are needed both to attract interest and to make them more accessible. While the potential for new ideas used in future research is difficult to assess, some use may be found here.

In this paper, the authors make use of the remodulization method developed in [1] as a vehicle to characterize the conditions under which solutions exist and then determine the solution space. The method is more efficient than those cited in the standard references. This novel approach relates the solution space of $cx \equiv a \bmod b$ to the Euler totient function for c rather than that

of b, which allows one to develop an alternative and somewhat more efficient approach to the problem of creating enciphering and deciphering keys in public-key cryptosystems.

Remodulization

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

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

The notation $x \equiv a \ mod \ b$, means 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 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,$\dots$,a_n,$b \in \mathbb{Z}$, then*

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

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

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

Proof. Write

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

and upon rewriting the columns,

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

and forming unions on the extended columns, the result follows.

This process is called remodulization by the factor c.

Linear Congruences

Theorem 2 *A linear congruence* $cx \equiv a \ mod \ b$, *where* $gcd(c, b) = 1$, *has as unique solution* $x \equiv a_0 \ mod \ b$, *where* $a_0 \in \{\frac{a+bk}{c}\}_{k=0}^{c-1}$.

Proof. Suppose one has the linear congruence,

$$cx \equiv a \bmod b \ ,$$

where $gcd(c, b) = 1$ and $0 < c < b$. (If c does not satisfy this requirement, then c may be reduced or augmented by some multiple of b so that it satisfies the condition $0 < c < b$.)

Remodulizing $a \ mod \ b$ by the factor c gives

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

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

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

it is seen that the only solvable linear congruence is

$$cx \equiv d \bmod cb \ .$$

The remaining linear congruences,

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

are not solvable, since in each case the factor c is pairwise relatively prime with the residues $\{a, a+b, \ldots , d-b, d+b, \ldots , a+b(c-1)\}$, and thus does not divide them.

For the solution $cx \equiv d \bmod cb$, however, dividing through by the factor c,

$$\frac{cx}{c} \equiv \frac{d}{c} \bmod \frac{cb}{c}$$

or,

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

Note that the Euclidean algorithm has not been invoked; all that was necessary to solve this problem was the fact that $gcd(c, b) = 1$. The theorem is illustrated by the following example.

Example 1 *Suppose* $12x \equiv 3$ *mod* 7*; this reduces to* $5x \equiv 3$ *mod* 7*. This linear congruence is solvable since* 3 *is divisible by* $gcd(5,7) = 1$*. Remodulizing* $3 \bmod 7$ *by the factor* 5 *gives*

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

so that

$$5x \equiv 10 \bmod 35$$

is the only possible solution and, upon dividing all three terms by 5,

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

Note that the remaining linear congruences $5x \equiv [3, 17, 24, 31] \bmod 35$ *do not admit any solutions, since in this example* $gcd(5, 35) = 5$ *does not divide any element in the set* $\{3, 17, 24, 31\}$*.*

Theorem 3 *If* $gcd(c, b) = d$ *and* $d|a$*, then the linear congruence* $cx \equiv a$ *mod* b*, has* d *distinct (incongruent) solutions modulo* b*.*

Proof. In the event $gcd(c, b) = d$, then a must be divisible by d, otherwise, the linear congruence will not admit integer solutions. With that in mind, write $c = c_0 d$, $a = a_0 d$, and $b = b_0 d$. If all three terms of the original linear congruence are divided by d,

$$c_0 x \equiv a_0 \bmod b_0 \ .$$

Since $gcd(c_0, b_0) = 1$, the resulting linear congruence has a solution $x \equiv x_0$ *mod* b_0. However, the modulus of the original congruence is $b = b_0 d$; therefore, by remodulizing the solution x_0 *mod* b_0 by the factor d one obtains

$$x \equiv [x_0, x_0 + b_0, \ldots , x_0 + b_0(d-1)] \bmod b_0 d \ .$$

Hence there are d distinct (incongruent) solutions *modulo* b to the linear congruence $cx \equiv a$ *mod* b if $gcd(c, b) = d$ and $d|a$. The theorem's utility is demonstrated by the following:

Example 2 *Suppose* $6x \equiv 9 \bmod 15$*. Dividing through by the common factor 3,* $2x \equiv 3 \bmod 5$*. This new linear congruence is solvable because 3 is divisible by* $gcd(2, 5) = 1$*. Using the remodulization method,* $2x \equiv [3, 8] \bmod 10$*, where the solution, by inspection, is* $x \equiv 4 \bmod 5$*. Then, remodulizing* $4 \bmod 5$ *by the factor 3, the solutions of the original linear congruence* $6x \equiv 9 \bmod 15$ *are* $x \equiv [4, 9, 14] \bmod 15$*.*

It is easily seen that the remodulization method is a trial-and-error method; however, after the solution is found, it is unnecessary to carry on any further computations. Another trial-and-error method consists of trying all residues of

the complete residue system $[1, 2, \ldots, b] \bmod b$ in the linear congruence $cx \equiv a \bmod b$ until the solution is found. In the case $c \ll b$, there are at most c computations using the remodulization method, compared to b possible computations of the alternate method.

Example 3 *Consider the linear congruence* $3x \equiv 5 \bmod 37$. *The remodulization method requires at most 3 steps, compared to 37 possible steps trying solutions of the complete residue system modulo* 37. *Remodulizing by the factor 3,* $3x \equiv [5, 42, \ldots] \bmod 111$. *By inspection, and requiring only 2 steps, the solution is* $x \equiv 14 \bmod 37$. *Performing the other calculation would have required 14 steps. Of course, simply guessing the solution may sometimes be just as fruitful. Picking an easy example is also helpful.*

A standard method of solving linear congruences involves Euler's phi function [2,3], or totient, denoted by Φ. The totient $\Phi(b)$ enumerates the positive integers less than b which are relatively prime to b. Euler's extension of Fermat's theorem states that

$$c^{\Phi(b)} \equiv 1 \bmod b \ ,$$

if $gcd(c, b) = 1$. Therefore, multiplying the linear congruence $cx \equiv a \bmod b$ through by the factor $c^{(\Phi(b)-1)}$ gives

$$c^{\Phi(b)}\, x \equiv a \cdot c^{(\Phi(b)-1)} \bmod b \ ,$$

or

$$x \equiv a \cdot c^{(\Phi(b)-1)} \bmod b \ .$$

Thus, finding the solution of the linear congruence $cx \equiv a \bmod b$ requires knowing $\Phi(b)$, or equivalently, the factorization of b.

The remodulization method predicts finding solutions of linear congruences based on the factor c, specifically $\Phi(c)$, rather than the modulus b. In cases dealing with very large integers, and where c is much less than b, or those cases in which the factorization of c is known, it may be more convenient to calculate the totient of c, rather than that of b.

Theorem 4 *The linear congruence* $cx \equiv a \bmod b$, *where* $gcd(c, b) = 1$, *has as solution*

$$x \equiv \left[\frac{a(1 - b^{\Phi(c)})}{c} \right] \bmod b \ .$$

Proof. Note that the linear congruence $cx \equiv a \bmod b$, where c and b are relatively prime and $0 < c < b$, implies the existence of integers x and y such that $cx - by = a$. Solving this equation instead for y, which is equivalent to

the linear congruence $by \equiv -a \bmod c$, shows that the solution, using Euler's theorem, is $y \equiv -a \cdot b^{(\Phi(c)-1)} \, mod \, c$. Substituting this result into $cx - by = a$, $cx = a + by = a + b\,[-a \cdot b^{(\Phi(c)-1)} \, mod \, c]$. Solving for x,

$$x \equiv \left[\frac{a + b\,[-a \cdot b^{(\Phi(c)-1)} \, mod \, c]}{c} \right] \bmod b \ ,$$

where $-a \cdot b^{(\Phi(c)-1)}$ is augmented by the proper multiple of c to obtain the least non-negative residue *modulo* c.

In the remodulization method, the elements $\{a, a+b, \ldots, a+b(c-1)\}$ are generated by $a + by$, for $y \in \{0, 1, 2, \ldots, c-1\}$. The $y + 1^{st}$ residue in the remodulized form $[a, a+b, \ldots, a+b(c-1)] \bmod bc$ is the solution, upon division by c.

If one is not interested in finding the least non-negative residue, the solution reduces to

$$x \equiv \left[\frac{a(1 - b^{\Phi(c)})}{c} \right] \bmod b \ .$$

Theorem 3 gives the obvious corollary to Theorem 4 in case $gcd(c, b) = d$.

Corollary 1 *If $gcd(c, b) = d$ and $d|a$, then the linear congruence $cx \equiv a \bmod b$ has d distinct solutions $x \equiv [x_0, x_0+b_0, \ldots, x_0+b_0(d-1)] \bmod b$, where $a = a_0 d$, $b = b_0 d$, $c = c_0 d$, and*

$$x_0 \equiv \left[\frac{a_0(1 - b_0^{\Phi(c_0)})}{c_0} \right] \bmod b_0 \ .$$

Remark 1 *If one solves the diophantine equation $cx + by = a$; i.e., $cx = a - by = a \bmod b$ formally, then the answer is $x = \frac{a}{c} - \frac{b}{c}y$, but the integer character and information is lost and not easily recovered. In the modular arithmetic format, however, the formula of Theorem 4 (or its corollary by Theorem 3) characterizes the countably infinitely many solutions.*

Applications

In public-key cryptosystems [2,4,5], an enciphering modulus m is created by multiplying two very large primes p and q, say $m = pq$; then one chooses an enciphering exponent e and a deciphering exponent d that satisfy the congruence relation

$$e \cdot d \equiv 1 \bmod \Phi(m) \ ,$$

where $gcd(e, \Phi(m)) = gcd(d, \Phi(m)) = 1$, and $\Phi(m) = (p-1)(q-1)$. By large, it is meant that the primes p and q should have 100 or more digits each. If one chooses the enciphering exponent e to be a prime such that $gcd(e, \Phi(m)) = 1$, then it is unnecessary to calculate $\Phi(\Phi(m))$ for the usual or standard solution

$$d \equiv e^{(\Phi(\Phi(m))-1)} \bmod \Phi(m) \ .$$

Instead, one only needs to calculate the solution

$$d \equiv \left[\frac{1 - \Phi(m)^{\Phi(e)}}{e}\right] \bmod \Phi(m) \ ,$$

where $\Phi(e) = e - 1$.

It is much easier (and more computationally efficient) to satisfy the condition $gcd(e, \Phi(m)) = 1$ than it is to calculate the prime decomposition of $\Phi(m)$ and its totient $\Phi(\Phi(m))$, even in those cases in which e is not prime but its factorization is known.

Example 4 *Suppose* $m = 7 \cdot 11 = 77$, *then* $\Phi(77) = 60$. *The problem is to find an enciphering exponent* e *and a deciphering exponent* d *which satisfy*

$$e \cdot d \equiv 1 \bmod 60 \ .$$

If one chooses $e = 13$, *then* d *is found by*

$$d \equiv \left[\frac{1 - 60^{\Phi(13)}}{13}\right] \bmod 60 \equiv \left[\frac{1 - 60^{12}}{13}\right] \bmod 60 \equiv 37 \bmod 60 \ ,$$

whereas $\Phi(\Phi(77)) = \Phi(60) = \Phi(2^2 \cdot 3 \cdot 5) = 16$. *Additionally, for* $e = 7$, $d = 43$; $e = 11$ *gives* $d = 11$; $e = 17$ *gives* $d = 53$; *and so on.*

This method may not supplant the Euclidean algorithm method. In order to extract a solution from the linear congruence $nx \equiv 1 \bmod m$, the Euclidean algorithm requires at most $\log_2(m)$ iterations, or in the case $n \ll m$, only $1 + \log_2(n)$ iterations. According to Bressoud [6], the method described here requires approximately the same number of iterations (perhaps one or two fewer), but since one is dealing with very large integers, i.e., $n \sim 10^{100}$ and $m \sim 10^{200}$, the difference is negligible. Therefore, those who have incorporated the Euclidean algorithm in their computer programs will not likely change to this method. Those just starting may well find this method preferable.

References

[1] Jeffrey F. Gold and Don H. Tucker, *Remodulization of Congruences*, Proceedings — National Conference on Undergraduate Research, University of North

Carolina Press, Asheville, North Carolina, 1992, Vol. II, 1036–41.

[2] David M. Burton, *Elementary Number Theory*, Second Edition, Wm. C. Brown Publishers, Iowa, 1989, 156–160, 175–179.

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

[4] David M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag New York, Inc., New York, 1989, 43–46.

[5] Kenneth H. Rosen, *Elementary Number Theory and Its Applications*, Third Edition, Addison-Wesley Publishing Company, Massachusetts, 1993, 253–264.

[6] David M. Bressoud. Personal communication.