5. Solving Linear Congruences

One of the goals in this chapter is to study the linear congruence \( ax \equiv b \pmod{n} \). In particular, we want to ask: (1) Existence (Are there any solutions?) (2) If so, how to solve it (Steps to solve the linear congruence)? (3) Number of Solutions (How many solutions are there)?

Remarks:

(1) If linear congruence \( ax \equiv b \pmod{n} \) has a solution, then there are always infinitely many solutions, because if \( x_0 \) is a solution, then \( x_0 + kn \) is also a solution for any integer \( k \). By mod \( n \), we can always assume that \( 0 \leq x_0 \leq n - 1 \). In other words, the solution of a linear congruence \( ax \equiv b \pmod{n} \), if it exists, will have the form \( x \equiv x_0 \pmod{n} \) where \( 0 \leq x_0 \leq n - 1 \). For example, the solutions to the linear congruence \( 23x \equiv 7 \pmod{91} \) are \( x \equiv 28 \pmod{91} \). In the following, when we talk about the solutions, or the number of solutions, we always mean that the solution modulo \( n \).

(2) We also recall some results in chapter 3: 
   \[ a \equiv b \pmod{n} \iff ac \equiv bc \pmod{cn} \]
   for any \( c \neq 0 \), multiplication law. If \( a \equiv b \pmod{n} \), then \( ac \equiv bc \pmod{n} \) for any \( c \), and the cancellation law if \( ac \equiv bc \pmod{n} \) and \( \gcd(c, n) = 1 \), where \( c \neq 0 \), then \( a \equiv b \pmod{n} \), i.e., if you want to divide \( c \) on both sides, you need to make sure that \( \gcd(c, n) = 1 \). The above results allow us to simplify a linear congruence \( ax \equiv b \pmod{n} \). For example, to solve \( 25x \equiv 20 \pmod{10} \), you only need to solve \( 5x \equiv 4 \pmod{2} \). To solve \( 25x \equiv 20 \pmod{3} \), by the cancellation law, you only need to solve \( 5x \equiv 4 \pmod{3} \) since \( \gcd(3, 5) = 1 \). However, warning, \( 25x \equiv 20 \pmod{5} \) is not equivalent to \( 5x \equiv 4 \pmod{5} \), so be careful.

Solving the linear congruence \( ax \equiv b \pmod{n} \) can be reduced to solve the linear Diophantine equation \( ax + nk = b \). Thus the theory in Chapter 2 about solving linear Diophantine equation can be applied here (recall, in chapter 2, the Steps of linear Diophantine equation \( ax + by = c \) with \( d|c \), where \( d = \gcd(a, b) \): 

**Step 1**: Use the reverse Euclidean Algorithm to find a single solution \((x_0, y_0)\) for the equation \( ax + by = d \) (where \( d = \gcd(a, b) \)); **Step 2**: Find a single solution (particular solution) \((\tilde{x}_0, \tilde{y}_0)\) for the equation \( ax + by = c \), by letting \( \tilde{x}_0 := \frac{c}{d}x_0, \tilde{y}_0 := \frac{c}{d}y_0 \), where \( d = \gcd(a, b) \); **Step 3**: The general integer solutions for the equation \( ax + by = c \) then are \( x = \tilde{x}_0 + (b/d)k, y = \tilde{y}_0 - k(a/d) \), where \( k \) is any integer (Note: If you can get \((x_0, y_0)\) by “inspection” directly, then you don’t need to go thorough the step 1 and step 2)).
• **Existence**: The linear congruence \( ax \equiv b \pmod{n} \) has a solution if and only if \( \gcd(a, n) \mid b \).

For example, consider the linear congruence \( 102x \equiv 37 \pmod{432} \). Since \( \gcd(102, 432) = 2 \) does not divide 37, there is no solution to \( 102x \equiv 37 \pmod{432} \).

• **Number of solutions**: The linear congruence \( ax \equiv b \pmod{n} \) with \( \gcd(a, n) \mid b \) has exactly \( d = \gcd(a, n) \) solutions modulo \( n \). In particular, there is exactly one solution modulo \( n \) to the linear congruence \( ax \equiv 1 \pmod{n} \) if \( \gcd(a, n) = 1 \).

For example, consider the linear congruence \( 23x \equiv 7 \pmod{91} \). Since \( \gcd(23, 91) = 1 \), it has only one solution modulo 91. For the linear congruence \( 35x \equiv 14 \pmod{84} \), \( \gcd(35, 84) = 7 \) and 7 \( \mid \) 14. So it has exactly 7 solutions modulo 84.

• **Steps** to solve the linear congruence \( ax \equiv b \pmod{n} \), assume that \( b = kd \) where \( d = \gcd(a, n) \):

  **Step 1**: Find a single solution \( x_0 \) for the linear congruence \( ax \equiv b \pmod{n} \), using the following observation: the linear congruence \( ax \equiv b \pmod{n} \) can be converted to the linear Diophantine equation \( ax + nk = b \) (see the discussion above).

  **Step 2**: If \( x_0 \) is a solution to \( ax \equiv b \pmod{n} \), then all the solutions have the form \( x = x_0 + m(n/d) \).

For example, Consider the linear congruence \( 35x \equiv 14 \pmod{84} \). \( \gcd(35, 84) = 7 \) and 7 \( \mid \) 14, so it has solutions (and from above, we know that it has exactly 7 solution modulo 84. We now follow the above steps to find them.

**Step 1**: Find a single solution \( x_0 \) the linear congruence \( 35x \equiv 14 \pmod{84} \) by converting it to the linear Diophantine equation \( 35x + 84k = 14 \), which is equivalent to \( 5x + 12k = 2 \). By the method discussed in chapter 2 (Steps of solving linear Diophantine equations) or by inspection, \( x_0 = -2 \) (and \( k = 1 \)) is an integer solution.

**Step 2**: All the solutions have the form \( x = -2 + m \times 12 \), where \( m \) is any integer (here we take \( n = 84, d = 7 \)). Obviously, we can take \( m = 1, \ldots, 6, 7 \) to get solutions which are between 0 to 83 (note that from the above, the solution
of a linear congruence \( ax \equiv b \pmod{n} \), if it exists, will have the form \( x \equiv x_0 \pmod{n} \) where \( 0 \leq x_0 \leq n - 1 \). They are \( x \equiv 10 \pmod{84} \), \( x \equiv 22 \pmod{84} \), \( x \equiv 34 \pmod{84} \), \( x \equiv 46 \pmod{84} \), \( x \equiv 58 \pmod{84} \), \( x \equiv 70 \pmod{84} \), \( x \equiv 82 \pmod{84} \). Note that, we know earlier that the linear congruence \( 35x \equiv 14 \pmod{84} \) has exactly 7 solution modulo 84.

Remark: As we discuss at the begining of the notes, you can simply the equation before you solve. Note that \( 35x \equiv 14 \pmod{84} \iff 5x \equiv 2 \pmod{12} \). So you can solve \( 5x \equiv 2 \pmod{12} \) instead to get solution (similar to above) \( x = -2 + m \times 12 \), where \( m \) is any integer. Then follow the above step, by take \( m = 1, \ldots, 6, 7 \), we get all solutions to the equation \( 35x \equiv 14 \pmod{84} \) as \( x \equiv 10 \pmod{84} \), \( x \equiv 22 \pmod{84} \), \( x \equiv 34 \pmod{84} \), \( x \equiv 46 \pmod{84} \), \( x \equiv 58 \pmod{84} \), \( x \equiv 70 \pmod{84} \), \( x \equiv 82 \pmod{84} \).

Example 2. Consider the linear congruence \( 23x \equiv 7 \pmod{91} \). Since \( \gcd(23, 91) = 1 \), there is a solution to \( 23x + 91y = 1 \). By the Euclidean Algorithm \( 91 = 4(23) - 1 \). Multiplying 7 on both sides yields (because we are looking for the solution to \( 23x \equiv 7 \pmod{91} \)) \( 91 \times 7 = 28 \times 23 - 7 \), i.e. \( 23 \times 28 \equiv 7 \pmod{91} \). Thus \( x_0 = 28 \) is a solution to the linear congruence \( 23x \equiv 7 \pmod{91} \). This finishes the step 1. From step 2, all the solutions have the form \( x = 28 + m \times 91 \), i.e. \( x \equiv 28 \pmod{91} \) is the only solution. Note that, we know earlier that the linear congruence \( 23x \equiv 7 \pmod{91} \) has only one solution modulo 91.

- **Multiplicative Inverse**: An integer \( x \) is said to be a *multiplicative inverse of a modulo n* if \( x \) satisfies \( ax \equiv 1 \pmod{n} \). For example, by solving \( 3x \equiv 1 \pmod{5} \), we get the multiplicative inverse of 3 modulo 5 is 2.

- **Theorem on the existence of multiplicative inverse**: Suppose that \( n > 0 \) be an integer. Then \( a \) has a multiplicative inverse modulo \( n \) if and only if \( \gcd(a, n) = 1 \).

- **Solving the system of two linear congruence** \( ax + by \equiv d \pmod{n} \), \( cx + dy \equiv f \pmod{n} \): \( x \equiv (ad - bc)^{-1}(de - bf) \pmod{n} \), \( y \equiv (ad - bc)^{-1}(af - ec) \pmod{n} \).
• **Factorials:**
  
  (1) For each integer $n > 0$, $n! \equiv n \pmod{n}$;
  
  (2) If $n$ is prime, then $(n - 2)! \equiv 1 \pmod{n}$;
  
  (3) If $n$ is prime, then $(n - 1)! \equiv n - 1 \pmod{n}$;
  
  (4) If $n = 4$, then $(n - 1)! \equiv 2 \pmod{n}$;
  
  (5) If $n \neq 4$ and $n$ is not prime, then $(n - 1)! \equiv 0 \pmod{n}$;

• **Wilson’s Theorem:** If $p$ is prime, then $(p - 1)! \equiv -1 \pmod{p}$. 
