Discrete Mathematics and Its Applications

4.4 Solving Congruences

Wenjing Li

wjli@bupt.edu.cn

School of Computer Science

Beijing University of Posts & Telecommunications

Solving Congruences

- **Definition:**
  - A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a ***linear congruence***.
  - Such congruences arise throughout number theory and its applications.

Solving Congruences

- How can we solve the linear congruence

$$ax \equiv b \pmod{m}?$$

- **Method:**
  - One method that we will describe uses an integer if such an integer exists. Such an integer $\bar{a}$ is said to be an **inverse of *a* modulo *m*** (*a模m的逆元*).

$$\bar{a}a \equiv 1 \pmod{m}$$

$$m \mid (\bar{a}a-1)$$

- **Example:**
  - find an inverse of 3 modulo 7.
  - since 5·3 = 15 ≡ 1 (mod 7), 5 is solution.

$$7 \mid (3x-1)$$

Inverse of a modulo m

- **Theorem 1:**
  - If *a* and *m* are relatively prime integers and *m* > 1, then an inverse of *a* modulo *m* exists.
  - Two integers *a* and *m* are relatively prime when

    $$gcd(a,m) = 1$$

  - This theorem guarantees that an inverse of *a* modulo *m* exists ***whenever a and m are relatively prime***.
  - Furthermore, this inverse is ***unique modulo m***. (This means that there is a unique positive integer $\bar{a}$ less than *m* that is an inverse of *a* modulo *m* and every other inverse of *a* modulo *m* is congruent to $\bar{a}$ modulo *m*.) (a模m的任何其他逆与该逆为模m的同余)

Inverse of a modulo m

- **Proof:**
  - **Existence:**
    - Since gcd(a, m) = 1, by Theorem 6 of Section 4.3 (**Bézout's Theorem**), there are integers s and t such that $sa + tm = 1$.
    - Hence, $sa + tm \equiv 1 \pmod{m}$.
    - Since $tm \equiv 0 \pmod{m}$, it follows that $\boldsymbol{sa} \equiv 1 \pmod{m}$
    - Consequently, ***s*** is an inverse of ***a*** modulo ***m***.

使用贝祖系数法可以求a模m的逆

INVERSE OF A MODULO M

- **Proof (cont):**
  - **Uniqueness (contradiction)**
    - Assume that there are two inverses of *a modulo m: b* and *c*
    - That is *b* and *c* satisfy the congruence $ax \equiv 1 \pmod{m}$.
    - i.e. $ab \equiv 1 \pmod{m}$ *and* $ac \equiv 1 \pmod{m}$
    - $\therefore ab \equiv ac \pmod{m}$
    - *and* $\gcd(a,m)=1$ *(premise)*
    - Use Theorem 7 of Section 4.3, $b \equiv c \pmod{m}$.

a模m的任何逆都是模m同余的

Finding Inverses

- The ***Euclidean algorithm and Bézout coefficients*** gives us a systematic approaches to finding inverses.
- **Example 1**: Find an inverse of 3 modulo 7.

$3x \equiv 1 \ (\mathrm{mod}\ 7)$

- **Solution**:
  - Because gcd(7, 3) = 1, by Theorem 1, an inverse of 3 modulo 7 exists.
  - Using the Euclidian algorithm: $7 = 2\cdot3 + 1$.
  - From this equation, we get $1= 1\cdot7-2\cdot3$, and see that 1 and −2 are Bézout coefficients of 7 and 3.
  - Hence, −2 is an inverse of 3 modulo 7.
  - Also every integer congruent to −2 modulo 7 is an inverse of 3 modulo 7, i.e., -9, 5, 12, etc.

Finding Inverses

- **Example 2:** Find an inverse of 101 modulo 4620.
- **Solution:**
  - First use the Euclidian algorithm to show that gcd(4620,101) = 1.
  - Then work backwards to get Bézout coefficients.

$\underline{4620 = 45\cdot 101 + 75}$

$\underline{101 = 1\cdot 75 + 26}$

$\underline{75 = 2\cdot 26 + 23}$

$\underline{26 = 1\cdot 23 + 3}$

$\underline{23 = 7\cdot 3 + 2}$

$\underline{3 = 1\cdot 2 + 1}$

$\underline{2 = 2\cdot 1}$

$\underline{1 = 3 - 1\cdot 2}$

$\underline{1 = 3 - 1\cdot(23 - 7\cdot 3) = - 1\cdot 23 + 8\cdot 3}$

$\underline{1 = -1\cdot 23 + 8\cdot(26 - 1\cdot 23) = 8\cdot 26 - 9\cdot 23}$

$\underline{1 = 8\cdot 26 - 9\cdot(75 - 2\cdot 26) = 26\cdot 26 - 9\cdot 75}$

$\underline{1 = 26\cdot(101 - 1\cdot 75) - 9\cdot 75}$

$\underline{\qquad = 26\cdot 101 - 35\cdot 75}$

$\underline{1 = 26\cdot 101 - 35\cdot(4620 - 45\cdot 101)}$

$\underline{\qquad = - 35\cdot 4620 + 1601\cdot 101}$

Using Inverses to Solve Congruences

- **Definition:**
  - We can solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$. ⇨ $x \equiv \bar{a} \cdot b \pmod{m}$
- **Example 3:**
  - What are the solutions of the congruence $3x \equiv 4 \pmod{7}$.
- **Solution:**
  - We found that −2 is an inverse of 3 modulo 7.
  - We multiply both sides of the congruence by −2 giving

    $-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}$. **(why?)**
  - Because $-6 \equiv 1 \pmod{7}$ and $-8 \equiv 6 \pmod{7}$
  - it follows that if x is a solution, then $x \equiv -8 \pmod{7} \equiv 6 \pmod{7}$

Using Inverses to Solve Congruences

- **Further more:**
  - We need to determine if every x with $x \equiv 6 \pmod{7}$ is a solution of $3x \equiv 4 \pmod{7}$.
  - By Theorem 5 of Section 4.1 (积同余定理), it follows that $3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod{7}$ which shows that all such x satisfy the congruence.
  - The solutions are the integers x such that $x \equiv 6 \pmod{7}$, namely, 6, 13, 20 … and −1, − 8, − 15,…

- **Exercise:** Solve the congruence using inverse of *a mod m*
  - $19x \equiv 4 \ (mod\ 141)$

The Chinese Remainder Theorem

- In the forth century, the Chinese mathematician Sun-Tsu asked:
  - There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?
- This puzzle can be translated into the solution of the system of congruences:
  - $x \equiv 2 \pmod{3}$,
  - $x \equiv 3 \pmod{5}$,
  - $x \equiv 2 \pmod{7}$?

南北朝时期《孙子算经》：
有物不知其数，三三数之剩二，
五五数之剩三，七七数之剩二。
问物几何？

- We’ll see how the theorem that is known as the ***Chinese Remainder Theorem*** can be used to solve Sun-Tsu’s problem.

The Chinese Remainder Theorem

- **Theorem 2: (*The Chinese Remainder Theorem:CRT*)**
  - Let $m_1, m_2, \ldots, m_n$ be ***pairwise relatively prime*** positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ be arbitrary integers. Then the system

    $x \equiv a_1 \ (\bmod\ m_1)$

    $x \equiv a_2 \ (\bmod\ m_2)$

    ….

    $x \equiv a_n \ (\bmod\ m_n)$

    has a unique solution modulo m while $\boldsymbol{m = m_1 m_2 \cdots m_n}$.
  - That is, there is a solution x with $0 \leq x < m$ and all other solutions are congruent modulo m to this solution.

- **Proof**:
  - We'll show that a solution exists by describing a way to construct the solution. Showing that the solution is unique modulo m is Exercise 30.

The Chinese Remainder Theorem

- **Proof: To construct a solution.**
  - First let $M_k = m/m_k$ for $k = 1,2,\ldots,n$ and $\mathbf{m = m_1 m_2 \cdots m_n}$.
  - Since $\gcd(m_k, M_k) = 1$, by Theorem 1, there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_k\, y_k \equiv 1 \ (\bmod\ m_k).$$

$$x = \left(\sum_{k=1}^{n} a_k M_k\, y_k\right) \bmod m$$

  - Form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n .$$

  - Let $x \bmod m_k$, note that because $M_j \equiv 0 \ (\bmod\ m_k)$ whenever $j \neq k$, all terms except the kth term in x are $\equiv 0 \ (\bmod\ m_k)$.
  - Because $M_k\, y_k \equiv 1 \ (\bmod\ m_k)$, we see that

$$x \equiv a_k M_k y_k \ (\bmod\ m_k) \equiv a_k \ (\bmod\ m_k), \ \text{for } k = 1,2,\ldots,n.$$

  - Hence, x is a simultaneous solution to the n congruences.
    - $x \equiv a_1 \ (\bmod\ m_1)$, $x \equiv a_2 \ (\bmod\ m_2)$, …. , $x \equiv a_n \ (\bmod\ m_n)$

The Chinese Remainder Theorem

$$x = (\sum_{k=1}^{n} a_k M_k\, y_k) \bmod m$$

- **Example 5:**
  - Consider the 3 congruences from Sun-Tsu's problem:

    $x \equiv 2 \ (\bmod 3)$, $x \equiv 3 \ (\bmod 5)$, $x \equiv 2 \ (\bmod 7)$.
  - Let $m = 3 \cdot 5 \cdot 7 = 105$,
  - Let $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$.
  - We see that $35 \cdot y_1 \equiv 1 \ (\bmod 3)$
    - $y_1=2$ is an inverse of $M_1 = 35$ modulo 3 since $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \ (\bmod 3)$
    - $y_2=1$ is an inverse of $M_2 = 21$ modulo 5 since $21 \equiv 1 \ (\bmod 5)$
    - $y_3=1$ is an inverse of $M_3 = 15$ modulo 7 since $15 \equiv 1 \ (\bmod 7)$
  - Hence, $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \ (mod\ 105)$

  $= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \ (mod\ 105) = 233 \ (mod\ 105) = 23 \ (mod\ 105)$
  - We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it! （can be used in privacy calculus)

Back Substitution

- **Definition:**
  - We can also solve systems of linear congruences with pairwise relatively prime moduli by rewriting a congruences as an equality using Theorem 4 in Section 4.1, substituting the value for the variable into another congruence, and continuing the process until we have worked through all the congruences.
  - This method is known as ***back substitution*** **(***反向替代/后向代入法***)**.

Let a,b ∈Z, m ∈Z⁺. Then:
a≡b (mod m) ⇔ ∃k ∈Z a=b+km.

- **Example 6**:
  - Use the method of back substitution to find all integers x such that

$$x \equiv 1 \pmod{5}, \quad x \equiv 2 \pmod{6}, \quad x \equiv 3 \pmod{7}.$$

Back Substitution

- **Solution:** ① $x \equiv 1 \pmod 5$, ② $x \equiv 2 \pmod 6$, ③ $x \equiv 3 \pmod 7$

1. By Theorem 4 in Section 4.1, the congruence ① can be rewritten as $x = 5t + 1$, where t is an integer.
2. Substituting into the congruence ② yields $5t + 1 \equiv 2 \pmod 6$.
3. Solving this tells us that $t \equiv 5 \pmod 6$.
4. Using Theorem 4 again gives $t = 6u + 5$ where u is an integer.
5. Substituting this back into $x = 5t + 1$,
   gives $x = 5(6u + 5) + 1 = 30u + 26$.
6. Inserting this into the equation ③, gives $30u + 26 \equiv 3 \pmod 7$.
7. Solving this congruence tells us that $u \equiv 6 \pmod 7$.
8. By Theorem 4, $u = 7v + 6$, where v is an integer.
9. Substituting this expression for u into $x = 30u + 26$, tells us that
   $x = 30(7v + 6) + 26 = 210v + 206$.
10. Translating this back into a congruence we find the solution
    $x \equiv 206 \pmod{210}$.

Computer Arithmetic with Large Integers

- **Definition:**
  - Suppose that $m_1, m_2, \ldots, m_n$ are pairwise relatively prime moduli and let m be their product.
  - By the **Chinese remainder theorem**, we can show that an integer a with $0 \le a < m$ can be uniquely represented by the n-tuple consisting of its remainders upon division by m_k, $k=1,2,\ldots,n$.

  (a可以唯一表示为一个n元组，每个数分别是模m_k的余数)

  - That is, we can uniquely represent a by

$$(a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_n).$$

Computer Arithmetic with Large Integers

- **Example 7:**
  - What are the pairs used to represent the nonnegative integers less than 12 when they are represented by the ordered pair where the first component is the remainder of the integer upon division by 3 and the second component is the remainder of the integer upon division by 4? (分别用模3和模4的余数表示出小于12的整数)

What are the benefits?

- **Solution:**
  - We have the following representations, obtained by finding the remainder of each integer when it is divided by 3 and by 4:

0=(0,0)

1=(1,1)

2=(2,2)

3=(0,3)

4=(1,0)

5=(2,1)

6=(0,2)

7=(1,3)

8=(2,0)

9 =(0,1)

10=(1,2)

11=(2,3)

Fermat's Little Theorem

- **Theorem 3:**
  - If *p* is prime and *a* is an integer not divisible by *p*, then

$$a^{p-1} \equiv 1 \ (mod\ p)$$

  - Furthermore, for every integer *a* we have

$$a^{p} \equiv a \ (mod\ p)$$

- **Example 9**: Find 7^{222} mod 11
  - By *Fermat's little theorem*, $7^{10} \equiv 1$ (mod 11)
  - $(7^{10})^{k} \equiv 1$ (mod 11), for every positive integer k. **(why?)**
  - $7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^{2} \equiv (1)^{22} \cdot 49 \equiv 5$ (mod 11).
  - 7^{222} mod 11 = 5.

一种特定的快速模指数计算方法

Pseudoprimes

- **Definition:**
  - By *Fermat's little theorem*, *n* > 2 is prime, where

    $$2^{n-1} \equiv 1 \pmod{n}.$$

  - But if this congruence holds, *n* may not be prime. Composite integers *n* such that $2^{n-1} \equiv 1 \pmod{n}$ are called ***pseudoprimes to the base 2***（基数2的伪素数/2为底的伪素数）.
- **Example 10:**
  - The integer 341 is a pseudoprime to the base 2.
    - $341 = 11 \cdot 31$
    - $2^{340} \equiv 1 \pmod{341}$ (*see in Exercise* 37)
  - Other pseudoprimes: 561, 645, 1105, 1387, 1729……

Pseudoprimes

- **Definition 1:**
  - We can replace 2 by any integer $b \geq 2$.
  - Let b be a positive integer.
  - If n is a composite integer, and $\boldsymbol{b^{n-1} \equiv 1 \pmod{n}}$, then n is called a ***pseudoprime to the base b***. （基数b的伪素数）

PSEUDOPRIMES

- Given a positive integer *n*, such that $2^{n-1} \equiv 1 \pmod{n}$:
  - If *n* does not satisfy the congruence, it is composite.
  - If *n* does satisfy the congruence, it is either prime or a pseudoprime to the base 2.
- Doing similar tests with additional bases *b*, provides more evidence as to whether *n* is prime.
- Among the positive integers not exceeding a positive real number *x*, compared to primes, there are relatively few pseudoprimes to the base *b*.
  - For example, among the positive integers less than 10^{10} there are 455,052,512 primes, but only 14,884 pseudoprimes to the base 2.

Carmichael Numbers (optional)

- **Definition 2:**
  - There are **composite integers *n*** that pass all tests with bases *b* such that gcd(*b*,*n*) = 1.
  - A composite integer *n* that satisfies the congruence $\boldsymbol{b^{n-1} \equiv 1 \pmod{n}}$ for all positive integers *b* with gcd(*b*,*n*) = 1 is called a ***Carmichael number***.

1. n是合数

2. 对于所有与n互质的数b而言，n都是伪素数

Robert Carmichael(1879-1967)

Carmichael Numbers (optional)

- **Example 11:** The integer 561 is a Carmichael number.
  - 561 is composite, since $561 = 3 \cdot 11 \cdot 17$.
  - If $\gcd(b, 561) = 1$, then $\gcd(b, 3) = 1$, $\gcd(b, 11) = 1$, $\gcd(b, 17) = 1$. **(why?)**
  - Using Fermat's Little Theorem:

    $b^2 \equiv 1 \pmod 3$, $b^{10} \equiv 1 \pmod{11}$, $b^{16} \equiv 1 \pmod{17}$.
  - Then

    $$b^{560} = (b^2)^{280} \equiv 1 \pmod 3,$$
    $$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11},$$
    $$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}.$$
  - It follows (*see Exercise* 29) that $b^{560} \equiv 1 \pmod{561}$ for all positive integers b with $\gcd(b,561) = 1$. Hence, 561 is a Carmichael number.

$b^{n-1} \equiv 1 \pmod n$, $b^{560} \equiv 1 \pmod{561}$

- Even though there are infinitely many Carmichael numbers, there are other tests (described in the exercises) that form the basis for efficient probabilistic primality testing. (*see Chapter* 7)

Primitive Roots（原根)

- **Definition 3**
  - A **primitive root** modulo a prime p is an integer r in Z_p, such that every **nonzero** element of Z_p is a power of r.
- **Example 12**
  - Determine whether 2 and 3 are primitive roots modulo 11.
  - Since every element of Z_{11} is a power of 2 mod 11, 2 is a primitive root of 11. Powers of 2 (modulo 11): $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$.
  - Since not all elements of Z_{11} are powers of 3, 3 is not a primitive root of 11. Powers of 3 (modulo 11): $3^1 = 3$, $3^2 = 9$, $3^3 = 5$, $3^4 = 4$, $3^5 = 1$, 3^6=3, and the pattern repeats for higher powers.

***p*为素数，若存在一个正整数*r*，使得 *r*, *r*^{2}, *r*^{3}, … , *r*$^{p-1}$ 模*p*互不同余，则称*r*为模*p*的一个原根**

There is a primitive root modulo *p* for every prime number *p*.

Discrete Logarithms (离散对数)

- **Definition 4**
  - Suppose that p is a prime, r is a primitive root modulo p, and a is an integer between 1 and $p-1$ inclusive (Z_p).
  - If $r^e \equiv a \ (mod\ p)$ and $0 \leq e \leq p-1$, we say that e is the **discrete logarithm** of a modulo p to the base r and we write $\boldsymbol{\log_r a = e}$ (where the prime p is understood).

Discrete Logarithms

- **Example 13:**

  $2^{?} = 3 \pmod{11}$

  - Find the discrete logarithms of 3 and 5 modulo 11 to the base 2.
    - **$2^8 = 3$ modulo 11.**
    - $\log_2 3 = 8$ the discrete logarithm of 3 modulo 11 to the base 2 is 8
    - **$2^4 = 5$ modulo 11.**
    - $\log_2 5 = 4$ the discrete logarithm of 5 modulo 11 to the base 2 is 4

- There is no known polynomial time algorithm for computing the discrete logarithm of a modulo p to the base r (when given the prime p, a root r modulo p, and a positive integer $a \in Z_p$).
- Finding discrete logarithms turns out to be **an extremely difficult** problem. The problem **plays a role in cryptography** as will be discussed in Section 4.6.

Homework

- **§ 4.4**
  - 6, 9, 12, 34.