4.4 Solving Congruences

Section Summary

- Linear Congruences
- The Chinese Remainder Theorem
- Computer Arithmetic with Large Integers
- Fermat's Little Theorem
- Pseudoprimes
- Primitive Roots and Discrete Logarithms

Linear 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.

  The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

One method of solving linear congruences makes use of an inverse $\bar{a}$, if it exists. Although we can not divide both sides of the congruence by a, we can multiply by $\bar{a}$ to solve for x.

- Definition: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of a modulo m.

Example: 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1 \pmod{7}$

Inverse of a modulo m

The following theorem guarantees that an inverse of *a* modulo *m* exists whenever *a* and *m* are relatively prime.

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

Proof: Since $\boldsymbol{gcd(a, m) = 1}$, by Theorem 6 of Section 4.3, there are integers *s* and *t* such that $sa + tm = 1$.

Hence, $sa + tm \equiv 1 \ (mod\ m)$.

Since $tm \equiv 0 \ (mod\ m)$, it follows $that\ sa \equiv 1 \ (mod\ m)$

Consequently, *s* is an inverse of *a* modulo *m*.

The uniqueness of the inverse is Exercise 7.

Finding Inverses1

The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

Example: Find an inverse of 3 modulo 7.

Solution: Because $\boldsymbol{gcd(3,7) = 1}$, by Theorem 1, an inverse of 3 modulo 7 exists.

Using the Euclidian algorithm: $7 = 2 \cdot 3 + 1$.

From this equation, we get $-2 \cdot 3 + 1 \cdot 7 = 1$, and see that -2 and 1 are Bézout coefficients of 3 and 7.

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., 5, -9, 12, etc.

Finding Inverses 2

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that gcd(101,4620) = 1.

$4620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

Since the last nonzero remainder is 1, gcd(101,4620) = 1

Working Backwards:

$1 = 3 - 1 \cdot 2$

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

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

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

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

$= 26 \cdot 101 - 35 \cdot 75$

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

$= -35 \cdot 4620 + 1601 \cdot 101$

Bézout coefficients : – 35 and 1601

1601 is an inverse of 101 modulo 4620

Using Inverses to Solve Congruences

We can solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

Example: What are the solutions of the congruence $3x \equiv 4 \pmod{7}$.

Solution: We found that -2 is an inverse of 3 modulo 7 (two slides back). We multiply both sides of the congruence by -2 giving $-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}$.

Because $-6 \equiv 1 \pmod{7}$ and $-8 \equiv 6 \pmod{7}$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 \pmod{7}$.

We need to determine if every x with $x \equiv 6 \pmod{7}$ is a solution. Assume that $x \equiv 6 \pmod{7}$. By Theorem 5 of Section 4.1, 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, $6, 13, 20 \ldots$ and $-1, -8, -15, \ldots$

The Chinese Remainder Theorem[1]

In the first 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:

$x \equiv 2 \pmod 3$,

$x \equiv 3 \pmod 5$,

$x \equiv 2 \pmod 7$?

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 Theorem2

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

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

...

$x \equiv a_n \pmod{m_n}$

has a unique solution modulo $m = m_1, m_2, \ldots, m_n$. (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 Theorem3

To construct a solution. First let $M_k = m/m_k$ for $k = 1, 2, \ldots, n$ and $m = m_1, m_2, \ldots, m_n$. 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

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

Form the sum

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

Note that because $M_j \equiv 0\ (mod\ m_k)$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k.

Because $M_k\, yk \equiv 1\ (mod\ mk_{)}$, we see that $x \equiv a_k M_k y_k \equiv a_k (mod\ m_k)$, for $k = 1, 2, \ldots, n$.

Hence, x is a simultaneous solution to the n congruences.

$$x \equiv a_1\ (mod\ m_1)$$
$$x \equiv a_2\ (mod\ m_2)$$
$$\ldots$$
$$x \equiv an\ (mod\ m_n)$$

The Chinese Remainder Theorem4

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

$x \equiv 2\ (mod\ 3),\ x \equiv 3\ (mod\ 5), x \equiv 2\ (mod\ 7).$

Let m = 3· 5 · 7 = 105, M_1 = m/3 = 35, M2 = m/5 = 21, M3 = m/7 = 15.

We see that

2 is an inverse of M_1 = 35 modulo 3 since $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1\ (mod\ 3)$

1 is an inverse of M_2 = 21 modulo 5 since $21 \equiv 1\ (mod\ 5)$

1 is an inverse of M_3 = 15 modulo 7 since $15 \equiv 1\ (mod\ 7)$

Hence,

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$$
$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23\ (mod\ 105)$$

We have shown that 23 is the smallest positive integer that is a simultaneous solution.

Check it!

Back Substitution

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.

Example: Use the method of back substitution to find all integers x such that $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.

Solution: By Theorem 4 in Section 4.1, the first congruence can be rewritten as $x = 5t + 1$, where t is an integer.

Substituting into the second congruence yields $5t + 1 \equiv 2 \pmod 6$.

Solving this tells us that $t \equiv 5 \pmod 6$.

Using Theorem 4 again gives $t = 6u + 5$ where u is an integer.

Substituting this back into $x = 5t + 1$, gives $x = 5(6u + 5) + 1 = 30u + 26$.

Inserting this into the third equation gives $30u + 26 \equiv 3 \pmod 7$.

Solving this congruence tells us that $u \equiv 6 \pmod 7$.

By Theorem 4, $u = 7v + 6$, where v is an integer.

Substituting this expression for u into $x = 30u + 26$, tells us that $x = 30(7v + 6) + 26 = 210u + 206$.

Translating this back into a congruence we find the solution $x \equiv 206 \pmod{210}$.

Computer Arithmetic with Large Integers$_1$

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 $0 \leq a < m$ can be uniquely represented by the n-tuple consisting of its remainders upon division by m_i, $i = 1, 2, \ldots, n$.

That is, we can uniquely represent a by

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

Example: **What are the pairs used to represent 10 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?**

Solution: **We have the following representations: 10 = (1, 2)**

Computer Arithmetic with Large Integers$_2$

To perform arithmetic with large integers, we select moduli $m_1, m_2, \ldots, m_n$, where each m_i is an integer greater than 2, gcd(m_i , m_j) = 1 whenever $i \neq j$, and $m = m_1 m_2 \cdots m_n$ is greater than the results of the arithmetic operations we want to carry out.

Method:

- **performing componentwise operations on the n-tuples representing these integers using their remainders upon division by m_i , $i = 1, 2, \ldots, n$.**
- **recover its value by solving a system of n congruences modulo m_i , i = 1, 2, … , n.**

The features of the method:

- **it can be used to perform arithmetic with integers larger than can ordinarily be carried out on a computer.**
- **computations with respect to the different moduli can be done in parallel, speeding up the arithmetic.**

Computer Arithmetic with Large Integers$_3$

Example: **Suppose that performing arithmetic with integers less than 100 on a certain processor is much quicker than doing arithmetic with larger integers. We can restrict almost all our computations to integers less than 100 if we represent integers using their remainders modulo pairwise relatively prime integers less than 100.**

Use the moduli of 99, 98, 97, and 95 to find the sum of 123,684 and 413,456.

Solution：

- **123,684 is represented as (33, 8, 9, 89), 413,456 is represented as (32, 92, 42, 16).**
- **(33, 8, 9, 89) + (32, 92, 42, 16) = (65 mod 99, 100 mod 98, 51 mod 97, 105 mod 95) = (65, 2, 51, 10).**
- **To find the sum, that is, the integer represented by (65, 2, 51, 10), we need to solve the system of congruences**

$$x \equiv 65 \pmod{99},\ x \equiv 2 \pmod{98},\ x \equiv 51 \pmod{97},\ x \equiv 10 \pmod{95}$$

- **537,140 is the unique nonnegative solution of this system less than 89,403,930. Consequently, 537,140 is the sum.**

Fermat's Little Theorem

Pierre de Fermat
(1601-1665)

Theorem 3: (Fermat's Little Theorem) If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$

Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$

(proof outlined in Exercise 19)

Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.

Example: Find $7^{222} \bmod 11$.

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$, for every positive integer k. Therefore,

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

Hence, $7^{222} \bmod 11 = 5$.

Pseudoprimes1

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.

Example: The integer 341 is a pseudoprime to the base 2.

$341 = 11 \cdot 31$

$2^{340} \equiv 1 \pmod{341}$ (*see in Exercise* 37)

We can replace 2 by any integer $b \geq 2$.

Definition: Let b be a positive integer. If n is a composite integer, and $b^{n-1} \equiv 1 \pmod{n}$, then n is called a pseudoprime to the base b.

Pseudoprimes$_2$

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

Robert Carmichael
(1879-1967)

There are composite integers n that pass all tests with bases b such that $\gcd(b,n) = 1$.

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

Example: **The integer 561 is a Carmichael number. To see this:**

561 is composite, since $561 = 3 \cdot 11 \cdot 13$.

If $\gcd(b, 561) = 1$, then $\gcd(b, 3) = \gcd(b, 11) = \gcd(b, 17) = 1$.

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.

Although 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)

Homework:

SE: P. 284 6(a,d), 10, 14, 20, 34

EE: P. 301 6(a,d), 10, 14, 20, 34