Chap 4.4 - Linear Congruences

**Definition:** A congruence of the form $ax \equiv b ( \mod m)$, 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 $ax \equiv b ( \mod m)$ are all integers $x$ that satisfy the congruence.

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

**Example:** What is the inverse of 3 modulo 7?

- 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 $x$. 

---

Announcements

- Read for next time Chap. 4.4-4.6
- Recitation Friday and Monday!
Inverse of $a$ modulo $m$

• The following theorem guarantees that an inverse of $a$ modulo $m$ exists whenever $a$ and $m$ are relatively prime. Two integers $a$ and $b$ are relatively prime when $\gcd(a,b) = 1$.

**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 $\hat{a}$ less than $m$ that is an inverse of $a$ modulo $m$ and every other inverse of $a$ modulo $m$ is congruent to $\hat{a}$ modulo $m$.)

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

---

Finding Inverses

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

**Example:** Find an inverse of 3 modulo 7.

**Solution:** Because $\gcd(3,7) = 1$, by Theorem 1, an inverse of 3 modulo 7 exists.
- Using the Euclidian algorithm to find $\gcd$: $7 = 2 \cdot 3 + 1$.
- 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

Example: Find an inverse of 101 modulo 4620.

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

Working Backwards:

\[
\begin{align*}
4620 &= 45 \cdot 101 + 75 \\
101 &= 1 \cdot 75 + 26 \\
75 &= 2 \cdot 26 + 23 \\
26 &= 1 \cdot 23 + 3 \\
23 &= 7 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 \\
1 &= 3 - 1 \cdot 2 \\
1 &= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\
1 &= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\
1 &= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75 \\
1 &= 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75 = 26 \cdot 101 - 35 \cdot 75 \\
1 &= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) = 26 \cdot 101 - 35 \cdot 4620 + 1601 \cdot 101 \\
1 &= -35 \cdot 4620 + 1601 \cdot 101 \\
\end{align*}
\]

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

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 \( a^{-1} \).

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

\[
-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7} \\
-6x \equiv -8 \pmod{7} \\
x = -8
\]

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 ... and \(-1, -8, -15,...\)

Plug in and check: \(3 \cdot (13) - 4 = 35 \text{ which is divisible by 7}\)

The Chinese Remainder Theorem

- 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:

\[
\begin{align*}
x &\equiv 2 \pmod{3}, \\
x &\equiv 3 \pmod{5}, \\
x &\equiv 2 \pmod{7}
\end{align*}
\]

- 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) 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
\[
x \equiv a_1 \pmod{m_1}
\]
\[
x \equiv a_2 \pmod{m_2}
\]
\[
\vdots
\]
\[
x \equiv a_n \pmod{m_n}
\]
has a unique solution modulo \( m = m_1 m_2 \cdots m_n \).

(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.

\[ \text{continued} \rightarrow \]

Example: Consider the 3 congruences from Sun-Tsu’s problem:
\[
x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}.\]
- Let \( m = 3 \cdot 5 \cdot 7 = 105, M_1 = m/3 = 35, M_3 = m/5 = 21, \)
  \( M_7 = m/7 = 15. \)
- We see that
  \[
  a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3
  \]
  \[
  = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233
  \]
  233 divided by 105 has remainder 23,
- We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!
The Chinese Remainder Theorem

• Did it work?
  1) \( x \equiv 2 \pmod{3} \)
  
  2) \( x \equiv 3 \pmod{5} \)
  
  3) \( x \equiv 2 \pmod{7} \)

Another way 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.

Another Way - Back Substitution (cont)

• Solution: By Theorem 4 in Section 4.1, the first congruence can be rewritten as \( x = 5t + 1 \), where \( t \) is an integer.
Another Way - Back Substitution (cont)

- **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 $t \equiv 3 \pmod{6}$.
  - $5t + 1 = 6t + 2$, this gives $t = -1$, but $t$ must be $> 0$, so take the next larger $t$ mod 6
  - So $t = -1 + 6 = 5$, so we know $t$ is congruent to 5 (mod 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 $30u + 26 \equiv 3 \pmod{7}$.
  - What could $u$ be? $30u + 26 = 7u + 3$, $23u = -23$ $u = -1$, need $u > 0$
  - Take the next $u$ mod 7, $-1 + 7 = 6$ $u = 6$
  - 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 $x = 30(7v + 6) + 26 = 210v + 206$.
Translation back into a congruence we find the solution $x \equiv 206 \pmod{210}$.

Check!

- $x \equiv 206 \pmod{210}$
- $x \equiv 1 \pmod{5}$
- $x \equiv 2 \pmod{6}$
- $x \equiv 3 \pmod{7}$

Fermat’s Little Theorem

**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 $7^{222} \pmod{11}$.

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,
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 \( a^p \equiv a \pmod{p} \).

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 \( 7^{222} \pmod{11} \).

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,

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

Hence, \( 7^{222} \pmod{11} = 5 \).

Pseudoprimes

- 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.

- 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

- 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.
Primitive Roots

**Definition:** A primitive root modulo a prime $p$ is an integer $r$ in $\mathbb{Z}_p$ such that every nonzero element of $\mathbb{Z}_p$ is a power of $r$.

**Example:** Since every element of $\mathbb{Z}_{11}$ is a power of 2, 2 is a primitive root of 11.

**Example:** Since not all elements of $\mathbb{Z}_{11}$ are powers of 3, 3 is not a primitive root of 11.

**Important Fact:** There is a primitive root modulo $p$ for every prime number $p$.

---

Discrete Logarithms

Suppose $p$ is prime and $r$ is a primitive root modulo $p$. If $a$ is an integer between 1 and $p-1$, that is an element of $\mathbb{Z}_p$, there is a unique exponent $e$ such that $r^e = a$ in $\mathbb{Z}_p$, that is, $r^e \mod p = a$.

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

**Example 1:** We write $\log_2 3 = 8$ since the discrete logarithm of 3 modulo 11 to the base 2 is 8 as $2^8 = 3 \mod 11$.

**Example 2:** We write $\log_2 5 = 4$ since the discrete logarithm of 5 modulo 11 to the base 2 is 4 as $2^4 = 5 \mod 11$.

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 $a \in \mathbb{Z}_p$). The problem plays a role in cryptography as will be discussed in Section 4.6.