4.4 Solving linear Congruences

After Mid-2 slides

Warm-up problem

Example: Use the Euclidean Algorithm to find the greatest common divisor of 52 and 180.

Then, use Bezout's Theorem/the "Reverse Euclidean Algorithm" to express gcd(52, 180) as a linear combination of 52 and 180. That is, find s and t such that $\gcd(52, 180) = 52s + 180t$

Euclidean Algorithm to find gcd(52, 180):

$180 = 52 \cdot 3 + 24$ (note that $52 \cdot 3 = 156$)

$52 = 24 \cdot 2 + 4$

$24 = 4 \cdot 6 + 0$

gcd = last nonzero remainder = **4**

Bezout's Theorem/ "reverse Euclidean Algorithm" gives:

$$\begin{aligned} \gcd(52, 180) &= 4 = 52 - 24 \cdot 2 \\ &= 52 - (180 - 52 \cdot 3) \cdot 2 \\ &= 52 - 2 \cdot 180 + 6 \cdot 52 \\ &= 7 \cdot 52 - 2 \cdot 180 \end{aligned}$$

Chap 4.4 - Linear Congruences

Definition: A congruence of the form

$$ax \equiv b(\bmod m),$$

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 $ax \equiv b(\bmod m)$ are all integers x that satisfy the congruence.

Definition: An integer $\bar{a}$ such that $\bar{a}a \equiv 1(\bmod m)$ 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.

Chap 4.4 - Linear Congruences

Definition: A congruence of the form

$$ax \equiv b(\bmod m),$$

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 $ax \equiv b(\bmod m)$ are all integers x that satisfy the congruence.

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

Example: What is the inverse of 3 modulo 7?

5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1(\bmod 7)$

- 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.

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

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

- Hence, $sa + tm \equiv 1 \pmod{m}$.
- Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$
- Consequently, s is an inverse of a modulo m.
- The uniqueness of the inverse is Exercise 7.

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 Euclidian algorithm to show that gcd(101,4620) = 1.

Working Backwards:

Finding Inverses

Example: Find an inverse of 101 modulo 4620.

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

Working Backwards:

$$4620 = 45\cdot101 + 75$$
$$101 = 1\cdot75 + 26$$
$$75 = 2\cdot26 + 23$$
$$26 = 1\cdot23 + 3$$
$$23 = 7\cdot3 + 2$$
$$3 = 1\cdot2 + 1$$
$$2 = 2\cdot1$$

$$1 = 3 - 1\cdot2$$
$$1 = 3 - 1\cdot(23 - 7\cdot3) = -1\cdot23 + 8\cdot3$$
$$1 = -1\cdot23 + 8\cdot(26 - 1\cdot23) = 8\cdot26 - 9\cdot23$$
$$1 = 8\cdot26 - 9\cdot(75 - 2\cdot26) = 26\cdot26 - 9\cdot75$$
$$1 = 26\cdot(101 - 1\cdot75) - 9\cdot75$$
$$= 26\cdot101 - 35\cdot75$$
$$1 = 26\cdot101 - 35\cdot(4620 - 45\cdot101)$$
$$= -35\cdot4620 + 1601\cdot101$$

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

Bézout coefficients : -35 and 1601

1601 is an inverse of 101 modulo 4620

Solving congruences

- The inverse of *a* is exactly the coefficient *s* from Bezout’s theorem, and we saw last time how to find such an *s*

Example: Determine the inverse of 19 modulo 141

Step 1: Do the Euclidean algorithm to confirm that gcd(19,141) = 1

Solving congruences

- The inverse of a is exactly the coefficient s from Bezout's theorem, and we saw last time how to find such an s

Example: Determine the inverse of 19 modulo 141

Step 1: Do the Euclidean algorithm to confirm that gcd(19,141) = 1

$$141 = 7 \cdot 19 + 8$$
$$19 = 2 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

Since the last remainder was 1, the Euclidean algorithm tells us that 19 and 141 are relatively prime, and theorem applies → there is an inverse of 19 (**mod** 141)

Solving congruences

- The inverse of *a* is exactly the coefficient *s* from Bezout's theorem, and we saw last time how to find such an *s*

Example: Determine the inverse of 19 modulo 141

Step 2: Do the Euclidean algorithm *in reverse* to find the coefficient on 19

$141 = 7 \cdot 19 + 8$

$19 = 2 \cdot 8 + 3$

$8 = 2 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

Solving congruences

- The inverse of *a* is exactly the coefficient *s* from Bezout's theorem, and we saw last time how to find such an *s*

Example: Determine the inverse of 19 modulo 141

Step 2: Do the Euclidean algorithm *in reverse* to find the coefficient on 19

$141 = 7 \cdot 19 + 8$
$19 = 2 \cdot 8 + 3$
$8 = 2 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

$$\boxed{\begin{aligned} 1 &= 3 - 1\cdot 2 \\ &= 3 - 1\cdot(8 - 2\cdot 3) \quad = 3 - 1\cdot 8 + 2\cdot 3 \quad = 3\cdot 3 - 1\cdot 8 \\ &= 3\cdot(19 - 2\cdot 8) - 1\cdot 8 \quad = 3\cdot 19 - 6\cdot 8 - 1\cdot 8 \quad = 3\cdot 19 - 7\cdot 8 \\ &= 3\cdot 19 - 7\cdot(141 - 7\cdot 19) \quad = 3\cdot 19 - 7\cdot 141 + 49\cdot 19 \\ &= \mathbf{52}\cdot 19 - 7\cdot 141 \end{aligned}}$$

$\Rightarrow$ So 52 is the inverse of 19 (**mod** 141)

Using Inverses to Solve Congruences

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

Example: What are the solutions of the congruence $3x \equiv 4(\bmod 7)$.

Using Inverses to Solve Congruences

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

Example: What are the solutions of the congruence $3x \equiv 4(\bmod 7)$.

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

$$-2 \cdot 3x \equiv -2 \cdot 4(\text{mod } 7).$$

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 $3x \equiv 3 \cdot 6 = 18 \equiv 4(\bmod 7)$ 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

- 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 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

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\;\;\vdots \\
x &\equiv a_n \pmod{m_n}
\end{aligned}
$$

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.

continued →

The Chinese Remainder Theorem

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

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

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Form the sum

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

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

Because $M_k y_k \equiv 1 \pmod{m_k}$, we see that $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, for $k = 1,2,\ldots,n$.

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

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

The Chinese Remainder Theorem

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

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

- Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_3 = m/5 = 21$, $M_3 = m/7 = 15$.
- We see that
- Hence,

The Chinese Remainder Theorem

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

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

- Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$.
- We see that
  - 2 is an inverse of $M_1 = 35$ modulo 3 since $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$
  - 1 is an inverse of $M_2 = 21$ modulo 5 since $21 \equiv 1 \pmod 5$
  - 1 is an inverse of $M_3 = 15$ modulo 7 since $15 \equiv 1 \pmod 7$
- Hence,

$$\begin{aligned} x &= a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \\ &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105} \end{aligned}$$

- 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 $x \equiv 206 \pmod{210}$.

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} **mod** 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 $a^{p-1} \equiv 1 \pmod{p}$

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} **mod** 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} **mod** $11 = 5$.