First Introduction

Our goal is to solve equations having the form $ax \equiv b \pmod{m}$. However, first we must discuss the last part of the previous section titled gcds as Linear Combinations

THEOREM 6 **BÉZOUT'S THEOREM** If a and b are positive integers, then there exist integers s and t such that $gcd(a,b) = sa + tb$.

DEFINITION 6 If a and b are positive integers, then s and t such that $gcd(a,b) = sa + tb$ are called $Bézout\ coefficients$ of a and b (after Étienne Bézout, a French mathematician of the eighteenth century). Also, the equation $gcd(a,b) = sa + tb$ is called $Bézout's\ identity$.

EXAMPLE 17 Express $gcd(252,198) = 18$ as a linear combination of 252 and 198.

Solution: To show that $gcd(252\,,198) = 18$, the Euclidean algorithm uses these divisions.

a		b		q		r	r		a		q		b
252	=	198	.	1	+	54	54	=	252	-	1	.	198
198	=	54	.	3	+	36	36	=	198	-	3	.	54
54	=	36	.	1	+	18	18	=	54	-	1	.	36

Starting with the last division, substitute the equation for the remainder in the previous division into the current computation.

Step		r		a		q		b
3	$18 = 4 \cdot (252 - 198) - 198$							
	$18 = 4 \cdot 252 - 5 \cdot 198$	**54**	=	252	-	1	.	198
2	$18 = 54 - (198 - 3 \cdot 54)$							
	$18 = 4 \cdot \mathbf{54} - 198$	**36**	=	198	-	3	.	54
1	$18 = 54 - \mathbf{36}$	18	=	54	-	1	.	36

Recall the $Bézout's\ identity\ gcd(a,b) = sa + tb$. In this example, we have $gcd(252,198) = 18$ and, hence, $s = 4$ and $t = -5$ making

$$18 = 4 \cdot 252 - 5 \cdot 198$$

completing the solution

Second Introduction

Solving linear congruences, which have the form $ax \equiv b \pmod{m}$, is an essential task in the study of number theory and its applications. To solve linear congruences, we employ inverses modulo m. We explain how to work backwards through steps of the Euclidean algorithm to find inverses modulo m. Once we have found an inverse of a modulo m, we solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides of the congruence by this inverse.

Linear Congruences

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**.

How can we solve the linear congruence $ax \equiv b \pmod{m}$, that is, how can we find all integers x that satisfy this congruence? One method that we will describe uses an integer $\overline{a}$ such that $\overline{a}\, a \equiv 1 \pmod{m}$, if such an integer exists. Such an integer $\overline{a}$ is said to be an inverse of a modulo m. Theorem 1 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. (That is, there is a unique positive integer $\overline{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\overline{a}$ modulo m.)

EXAMPLE 1

Find an inverse of 3 modulo 7 by first finding Bézout coefficients of 3 and 7. (Note that we have already shown that 5 is an inverse of 3 modulo 7 by inspection.)

Solution: Because $gcd(3,7) = 1$, Theorem 1 tells us that an inverse of 3 modulo 7 exists. The Euclidean algorithm ends quickly when used to find the greatest common divisor of 3 and 7.

$$7 = 2 \cdot 3 + 1$$

From this equation we see that

$$-2 \cdot 3 + 1 \cdot 7 = 1$$

Recall that $gcd(a, b) = sa + tb$ defines s and t as Bézout coefficients. This shows that -2 and 1 are Bézout coefficients of 3 and 7. We see that -2 is an inverse of 3 modulo 7. Note that every integer congruent to -2 modulo 7 is also an inverse of 3, such as 5, -9, 12, and so on.

EXAMPLE 2 Find an inverse of 101 modulo 4620.

Solution: For completeness, we present all steps used to compute an inverse of 101 modulo 4620. (Only the last step goes beyond methods developed in section 4.3 and illustrated in Example 17 in that section.) First, we use the Euclidean algorithm to show that $gcd(101,4620) = 1$. Then we will reverse the steps to find Bézout coefficients a and b such that $101a + 4620b = 1$. It will then follow that a is an inverse of 101 modulo 4620. The steps used by the Euclidean algorithm to find $gcd(101,4620)$ are

a		b		q		r	r		a		q		b
4620	=	101	.	45	+	75	75	=	4620	-	45	.	101
101	=	75	.	1	+	26	26	=	101	-	1	.	75
75	=	26	.	2	+	23	23	=	75	-	2	.	26
26	=	23	.	1	+	3	3	=	26	-	1	.	23
23	=	3	.	7	+	2	2	=	23	-	7	.	3
3	=	2	.	1	+	1	1	=	3	-	1	.	2

Because the last nonzero remainder is 1, we know that $gcd(101,4620) = 1$. We can now find the Bézout coefficients for 101 and 4620 by working backwards through these steps, expressing $gcd(101,4620) = 1$ in terms of each successive pair of remainders. In each step we eliminate the ***remainder*** by expressing it as a linear combination of the ***divisor*** and the ***dividend***. We obtain

Step		r		a		q		b
6	$1 = 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$							
	$1 = 1601 \cdot 101 - 35 \cdot 4620$	**75**	=	4620	-	45	.	101
5	$1 = 26 \cdot (101 - 75) - 9 \cdot 75$							
	$1 = 26 \cdot 101 - 35 \cdot \mathbf{75}$	**26**	=	101	-	1	.	75
4	$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26)$							
	$1 = 26 \cdot \mathbf{26} - 9 \cdot 75$	**23**	=	75	-	2	.	26
3	$1 = 8 \cdot (26 - 23) - 23$							
	$1 = 8 \cdot 26 - 9 \cdot \mathbf{23}$	**3**	=	26	-	1	.	23
2	$1 = 3 - 1 \cdot (23 - 7 \cdot 3)$							
	$1 = 8 \cdot \mathbf{3} - 1 \cdot 23$	**2**	=	23	-	7	.	3
1	$1 = 3 - 1 \cdot \mathbf{2}$	**1**	=	3	-	1	.	2

$$\mathbf{1601 \cdot 101 - 35 \cdot 4620 = 1}$$

That $\mathbf{1601 \cdot 101 - 35 \cdot 4620 = 1}$ tells us that $\mathbf{1601}$ and -35 are Bézout coefficients of 101 and 4620, and $\mathbf{1601}$ is an inverse of 101 modulo 4620.

EXAMPLE 2.1 Find an inverse of 4 modulo 9.

Solution: First, we use the Euclidean algorithm to show that $gcd(4,9) = 1$. Then we will reverse the steps to find Bézout coefficients s and t such that $s4 + t9 = 1$. It will then follow that s is an inverse of 4 modulo 9. The steps used by the Euclidean algorithm to find $gcd(4,9)$ are

Dividend		Divisor		Quotient		Remainder
9	=	4	.	2	+	1
4	=	1	.	4	+	0

$$1 = \mathbf{1} \cdot 9 - \mathbf{2} \cdot 4$$

That $1 = \mathbf{1} \cdot 9 - \mathbf{2} \cdot 4$ tells us that $\mathbf{1}$ and $\mathbf{-2}$ are Bézout coefficients of 9 and 4, and $\mathbf{-2}$ is an inverse of 4 modulo 9. Inverses of 4 modulo 9 are $\mathbf{-2 + k \cdot 9 = \cdots, -20, -11, -2, 7, 16, 25, \cdots}$

EXAMPLE 2.2 Find an inverse of 19 modulo 141.

Solution: First, we use the Euclidean algorithm to show that $gcd(19,141) = 1$. Then we will reverse the steps to find Bézout coefficients s and t such that $s19 + t141 = 1$. It will then follow that s is an inverse of 19 modulo 141. The steps used by the Euclidean algorithm to find $gcd(19,141)$ are

a		b		q		r
141	=	19	.	7	+	8
19	=	8	.	2	+	3
8	=	3	.	2	+	2
3	=	2	.	1	+	1

r		a		q		b
8	=	141	-	19	.	7
3	=	19	-	8	.	2
2	=	8	-	3	.	2
1	=	3	-	2	.	1

Step		r		a		q		b
4	$1 = 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19)$							
	$1 = 52 \cdot 19 - 7 \cdot 141$	**8**	=	141	-	19	.	7
3	$1 = 3 \cdot (19 - 2 \cdot 8) - 8$							
	$1 = 3 \cdot 19 - 7 \cdot \mathbf{8}$	**3**	=	19	-	8	.	2
2	$1 = 3 - (8 - 3 \cdot 2)$							
	$1 = 3 \cdot \mathbf{3} - 8$	**2**	=	8	-	3	.	2
1	$1 = 3 - \mathbf{2}$	**1**	=	3	-	2	.	1

$$1 = \mathbf{52} \cdot 19 - 7 \cdot 141$$

That $1 = \mathbf{52} \cdot 19 - \mathbf{7} \cdot 141$ tells us that $\mathbf{52}$ and $\mathbf{-7}$ are Bézout coefficients of 19 and 141, and $\mathbf{52}$ is an inverse of 19 modulo 141. Inverses of 19 modulo 141 are $\mathbf{52 + k \cdot 141 = \cdots, -89, 52, 193, \cdots}$

EXAMPLE 2.3 Find an inverse of 55 modulo 89.

Solution: First, we use the Euclidean algorithm to show that $gcd(55,89) = 1$. Then we will reverse the steps to find Bézout coefficients s and t such that $s55 + t89 = 1$. It will then follow that s is an inverse of 55 modulo 89. The steps used by the Euclidean algorithm to find $gcd(55,89)$ are

a		b		q		r	r		a		q		b
89	=	55	.	1	+	34	34	=	89	-	1	.	55
55	=	34	.	1	+	21	21	=	55	-	1	.	34
34	=	21	.	1	+	13	13	=	34	-	1	.	21
21	=	13	.	1	+	8	8	=	21	-	1	.	13
13	=	8	.	1	+	5	5	=	13	-	1	.	8
8	=	5	.	1	+	3	3	=	8	-	1	.	5
5	=	3	.	1	+	2	2	=	5	-	1	.	3
3	=	2	.	1	+	1	1	=	3	-	1	.	2

Step		r		a		q		b
	$1 = 13 \cdot 55 - 21 \cdot (89 - 55)$							
8	$1 = 34 \cdot 55 - 21 \cdot 89$	**34**	=	89	-	1	.	55
	$1 = 13 \cdot (55 - 34) - 8 \cdot 34$							
7	$1 = 13 \cdot 55 - 21 \cdot \mathbf{34}$	**21**	=	55	-	1	.	34
	$1 = 5 \cdot 21 - 8 \cdot (34 - 21)$							
6	$1 = 13 \cdot \mathbf{21} - 8 \cdot 34$	**13**	=	34	-	1	.	21
	$1 = 5 \cdot (21 - 13) - 3 \cdot 13$							
5	$1 = 5 \cdot 21 - 8 \cdot \mathbf{13}$	**8**	=	21	-	1	.	13
	$1 = 2 \cdot 8 - 3 \cdot (13 - 8)$							
4	$1 = 5 \cdot \mathbf{8} - 3 \cdot 13$	**5**	=	13	-	1	.	8
	$1 = 2 \cdot (8 - 5) - 5$							
3	$1 = 2 \cdot 8 - 3 \cdot \mathbf{5}$	**3**	=	8	-	1	.	5
	$1 = 3 - (5 - 3)$							
2	$1 = 2 \cdot \mathbf{3} - 5$	**2**	=	5	-	1	.	3
1	$1 = 3 - \mathbf{2}$	**1**	=	3	-	1	.	2

$$1 = \mathbf{34} \cdot 55 - 21 \cdot 89$$

That $1 = \mathbf{34} \cdot 55 - \mathbf{21} \cdot 89$ tells us that $\mathbf{34}$ and $-\mathbf{21}$ are Bézout coefficients of 55 and 89, and $\mathbf{34}$ is an inverse of 55 modulo 89. Inverses of 55 modulo 89 are $\mathbf{34} + \boldsymbol{k} \cdot \mathbf{89} = \cdots, \mathbf{-55}, \mathbf{34}, \mathbf{123}, \cdots$

Once we have an inverse $\overline{a}$ of a modulo m, we can solve the congruence $ax \equiv b (\mathbf{mod}\ m)$ by multiplying both sides of the linear congruence by $\overline{a}$, as Example 3 illustrates.

EXAMPLE 3 What are the solutions of the linear congruence $3x \equiv 4 \ (\mathbf{mod}\ 7)$?
Solution: By Example 1 we know that -2 is an inverse of 3 modulo 7.
Recall $gcd(3,7) = -2 \cdot 3 + 1 \cdot 7 = 1$ from example 1. Additional inverse values include 5, 12, … Let us select the ***first positive inverse*** value, 5. In the congruence

$$ax \equiv b(\mathbf{mod}\ m)$$

If $\overline{b}$ is an inverse of b modulo m, then

$$x = (\overline{b} \cdot b - m)\ \mathbf{mod}\ m$$
$$x = (5 \cdot 4 - 7)\ \mathbf{mod}\ 7 = 6$$

Applying our finding, we have

$$3x \equiv 3 \cdot 6 = 18 \equiv 4(\ \mathbf{mod}\ 7)$$

which shows that all such x satisfy the congruence. We conclude that the solutions to the congruence are integers x such that $x \equiv 6 \ (\mathbf{mod}\ 7)$, namely, $6, 13, 20, \ldots$, and $-1, -8, -15, \ldots$.

Test: Does $x = -8$ satisfy the congruence, $3x \equiv 4 \ (\mathbf{mod}\ 7)$? Is $-24 \equiv 4 \ (\mathbf{mod}\ 7)$? Recall the definition of congruence. We say that $a \equiv b(\mathbf{mod}\ m)$ if $m|(a - b)$. Does $7|(-24 - 4)$? Answer, yes.

EXAMPLE 3.1 Let us try another example. What are the solutions of the linear congruence $19x \equiv 4 \ (\mathbf{mod}\ 141)$?
Solution: From Example 2.2, we know that 52 is an inverse of 19 modulo 141

$$ax \equiv b(\mathbf{mod}\ m)$$

If $\overline{b}$ is an inverse of b modulo m, then

$$x = (\overline{b} \cdot b - m)\ \mathbf{mod}\ m$$
$$x = (52 \cdot 4 - 141)\ \mathbf{mod}\ 141 = 67$$

Applying our finding, we have

$$19x \equiv 19 \cdot 67 = 1273 \equiv 4(\ \mathbf{mod}\ 141)$$

which shows that all such x satisfy the congruence. We conclude that the solutions to the congruence are integers x such that $x \equiv 67 \ (\mathbf{mod}\ 141)$, namely, $67, 208, 349, \ldots$, and $-74, -215, -356, \ldots$.

Test: Does $x = -74$ satisfy the congruence, $19x \equiv 4 \ (\mathbf{mod}\ 141)$? Is $-1406 \equiv 4 \ (\mathbf{mod}\ 141)$? Recall the definition of congruence. We say that $a \equiv b(\mathbf{mod}\ m)$ if $m|(a - b)$. Does $141|(-1406 - 4)$? Answer, yes. $\frac{-1406-4}{141} = 10$

The Chinese Remainder Theorem

EXAMPLE 4 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; and when divided by 7, the remainder is 2. What will be the number of things?

This puzzle can be translated into the following question: What are the solutions of the systems of congruences

$$x \equiv 2 \ (\mathbf{mod}\ 3),$$
$$x \equiv 3 \ (\mathbf{mod}\ 5),$$
$$x \equiv 2 \ (\mathbf{mod}\ 7)?$$

We will solve this system, and with it Sun-Tsu's puzzle, later in this section.

THEOREM 2 **THE CHINESE REMAINDER THEOREM** Let $m\_1, m\_2, \cdots, m\_n$ be pairwise relatively prime positive integers greater than one and $a\_1, a\_2, \cdots, a\_n$ arbitrary integers. Then the system

$$x \equiv a\_1 \ (\mathbf{mod}\ m\_1),$$
$$x \equiv a\_2 \ (\mathbf{mod}\ m\_2),$$
$$\vdots$$
$$x \equiv a\_n \ (\mathbf{mod}\ m\_n)$$

has a unique solution modulo $m = m\_1\, m\_2 \cdots m\_n$. (That is, there is a solution x with $0 \le x < m$, and all other solutions are congruent modulo m to this solution.)

***Proof*:** To establish this theorem, we need to show that a solution exists and that it is unique modulo m. We will show that a solution exists by describing a way to construct this solution.

To construct a simultaneous solution, first let

$$M\_k = m/m\_k$$

for $k = 1,2,\cdots,n$. That is, M_k is the product of the moduli except for m_k. Because m_i and m_k have no common factors greater than 1 when $i \neq k$, it follows that $gcd(m\_k, M\_k) = 1$. Consequently, by Theorem 1, we know that there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M\_k\, y\_k \equiv 1 \ (\mathbf{mod}\ m\_k)$$

To construct a simultaneous solution, form the sum

$$x = a\_1\, M\_1\, y\_1 + a\_2\, M\_2\, y\_2 + \cdots + a\_n\, M\_n\, y\_n$$

Will now show that x is a simultaneous solution. First, note that because $M\_j \equiv 0(\mathbf{mod}\ m\_k)$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k. Because $M\_k\ y\_k \equiv 1\ (\mathbf{mod}\ m\_k)$ we see that

$$x \equiv a\_k\ M\_k\ y\_k \equiv a\_k\ \ (\mathbf{mod}\ m\_k\ ),$$

for $k = 1,2,\cdots,n$. We have shown that x is a simultaneous solution to the n congruences.

EXAMPLE 5

$x \equiv 2\ (\mathbf{mod}\ 3)$,
$x \equiv 3\ (\mathbf{mod}\ 5)$,
$x \equiv 2\ (\mathbf{mod}\ 7)$?

To solve the system of congruences in Example 4, first let $m = 3 \cdot 5 \cdot 7 = 105, M\_1 = m/3 = 35, M\_2 = m/5 = 21$, and $M\_3 = m/7 = 15$.

Find an inverse of 35 modulo 3.

a		b		q		r		r		a		q		b
35	=	3	.	11	+	2		2	=	35	-	11	.	3
3	=	2	.	1	+	1		1	=	3	-	1	.	2

Step		r		a		q		b
2	$1 = 3 - (35 - 3 \cdot 11)$							
	$1 = 12 \cdot 3 - 35$	2	=	35	-	11	.	3
1	$1 = 3 - 2$	1	=	3	-	1	.	2

Because $1 = -1 \cdot 35 + 12 \cdot 3$, we can find inverses of 35 modulo 3 equal $\cdots\ -4, -1, 2, 5. \cdots$ Select the ***first positive inverse*** of $M\_1 = 35$ modulo 3: The first positive inverse is **2**.

Find an inverse of 21 modulo 5.
By inspection, we find $1 = 21 - 4 \cdot 5$. $\mathbf{1}$ is an inverse of $M\_2 = 21$ modulo 5.

Find and inverse of 15 modulo 7.
By inspection, we find $1 = 15 - 2 \cdot 7$. $\mathbf{1}$ is an inverse of $M\_3 = 15$ modulo 7.

The solutions to this system are those x such that

$$\begin{aligned} x &\equiv a\_1\ M\_1\ y\_1 + a\_2\ M\_2\ y\_2 + a\_3\ M\_3\ y\_3 \\ &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \\ &= 233 \equiv 23(\mathbf{mod}\ 105), \end{aligned}$$

It follows that 23 is the smallest positive integer that is a simultaneous solution. We conclude that 23 is the smallest positive integer that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7.

EXAMPLE 6 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 an equality, $x = 5t + 1$ where t is an integer. Substituting this expression for x into the second congruence tells us that

$$5t + 1 \equiv 2 \pmod 6,$$

which can be easily solved to show that $t \equiv 5 \pmod 6$ (as the reader should verify). Using Theorem 4 in Section 4.1 again, we see that $t = 6u + 5$ where u is an integer. Substituting this expression for t into the equation $x = 5t + 1$ tells us that $x = 5(6u + 5) + 1 = 30u + 26$. We insert this into the third equation to obtain

$$30u + 26 \equiv 3 \pmod 7$$

Solving this congruence tells us that $u = 6 \pmod 7$ (as the reader should verify). Theorem 4 in Section 4.1 tells us that $u = 7v + 6$ where v is an integer. Substituting this expression for u into the equation $x = 30u + 26$ tells us that $x = 30(7v + 6) + 26 = 210u + 206$. Translating this back into a congruence, we find the solution to the simultaneous congruences,

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

Computer Arithmetic with Large Integers

Read for yourself.

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

$$a^p \equiv a \pmod p.$$

EXAMPLE 9 Find $7^{222} \bmod 11$.

Solution: We can use Fermat's little theorem to evaluate $7^{222} \bmod 11$ rather than using the fast modular exponentiation algorithm. By Fermat's little theorem we know that $7^{10} = 1 (\bmod 11)$, so $(7^{10})^k = 1 (\bmod 11)$ for every integer k. To take advantage of this last congruence, we divide the exponent 222 by 10, finding that $222 = 22 \cdot 10 + 2$. We now see that

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

It follows that $7^{222} \bmod 11 = 5$.

Primitive Roots and Discrete Logarithms.

Read for yourself.