الجامعة اللبنانية
كلية الإعلام والتوثيق

Chapter 3

Lecture : Exercises & Correction

Prepared by:

- Dr. Abbas Rammal
- Dr. Rabih Assaf

EX 19.

Find an inverse of a modulo m for each of these pairs of relatively prime integers using the method followed in Example 2.

a) $a = 4, m = 9$

b) $a = 19, m = 141$

c) $a = 55, m = 89$

d) $a = 89, m = 232$

(a) The **inverse** of a modulo m is an integer b for which $ab \equiv 1 \pmod{m}$

$$a = 4$$
$$m = 9$$

First perform the Euclidean algorithm:

$$9 = 2 \cdot 4 + 1$$
$$4 = 4 \cdot 1$$

The greatest common divisor is then the last nonzero remainder: $gcd(a, m) = 1$.

Next we write the greatest common divisor as a multiple of a and m:

$$\begin{aligned} gcd(a, m) &= 1 \\ &= 9 - 2 \cdot 4 \\ &= 1 \cdot 9 - 2 \cdot 4 \end{aligned}$$

The inverse is then the coefficient of a, which is -2.

Since $-2 \textbf{ mod } 9 = 7 \textbf{ mod } 9$, 7 is also the inverse of a modulo m.

(b) The **inverse** of a modulo m is an integer b for which $ab \equiv 1 \pmod{m}$

$$a = 19$$
$$m = 141$$

First perform the Euclidean algorithm:

$$\begin{aligned} 141 &= 7 \cdot 19 + 8 \\ 19 &= 2 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

The greatest common divisor is then the last nonzero remainder: $gcd(a, m) = 1$.

Next we write the greatest common divisor as a multiple of a and m:

$$\begin{aligned} gcd(a, m) &= 1 \\ &= 3 - 1 \cdot 2 \\ &= 1 \cdot 3 - 1 \cdot 2 \\ &= 1 \cdot 3 - 1 \cdot (8 - 2 \cdot 3) \\ &= 3 \cdot 3 - 1 \cdot 8 \\ &= 3 \cdot (19 - 2 \cdot 8) - 1 \cdot 8 \\ &= 3 \cdot 19 - 7 \cdot 8 \\ &= 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19) \\ &= 52 \cdot 19 - 7 \cdot 141 \end{aligned}$$

The inverse is then the coefficient of a, which is thus 52.

(c) The **inverse** of a modulo m is an integer b for which $ab \equiv 1 \pmod{m}$

$$a = 55$$
$$m = 89$$

First perform the Euclidean algorithm:

$$\begin{aligned}
89 &= 1 \cdot 55 + 34 \\
55 &= 1 \cdot 34 + 21 \\
34 &= 1 \cdot 21 + 13 \\
21 &= 1 \cdot 13 + 8 \\
13 &= 1 \cdot 8 + 5 \\
8 &= 1 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{aligned}$$

The greatest common divisor is then the last nonzero remainder: $gcd(a, m) = 1$.

Next we write the greatest common divisor as a multiple of a and m:

$$\begin{aligned}
gcd(a, m) &= 1 \\
&= 3 - 1 \cdot 2 \\
&= 1 \cdot 3 - 1 \cdot 2 \\
&= 1 \cdot 3 - 1 \cdot (5 - 1 \cdot 3) \\
&= 2 \cdot 3 - 1 \cdot 5 \\
&= 2 \cdot (8 - 1 \cdot 5) - 1 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8) \\
&= 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 1 \cdot 13) - 3 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21) \\
&= 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (55 - 1 \cdot 34) - 8 \cdot 34 \\
&= 13 \cdot 55 - 21 \cdot 34 \\
&= 13 \cdot 55 - 21 \cdot (89 - 1 \cdot 55) \\
&= 34 \cdot 55 - 21 \cdot 89
\end{aligned}$$

The inverse is then the coefficient of a, which is thus 34.

EX 20.

Solve the congruence $4x \equiv 5 \pmod{9}$ using the inverse of 4 modulo 9 found in part (a) of Exercise 5.

Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 5.

a) $19x \equiv 4 \pmod{141}$
b) $55x \equiv 34 \pmod{89}$
c) $89x \equiv 2 \pmod{232}$

$$4x \equiv 5 (\mathrm{mod}\ 9)$$

We use Bezout's Theorem to express gcd(9,4) as a lineal combination of 9 and 4. Thus, we can observe that the inverse of 4 is -2, but if we add 9 to -2, we obtain 7, so the inverse is, as well, 7.

$$9 = (2 * 4) + 1$$

so...

$$1 = (9 * 1) - (2 * 4) = (9 * 1) + ((-2) * 4)$$

So we can multiply both sides by 7 to obtain that x is equivalent with 8 mod 9.

$$7 * 4x \equiv 7 * 5 (\mathrm{mod}\ 9)$$
$$x \equiv 35 (\mathrm{mod}\ 9)$$
$$x \equiv 8 (\mathrm{mod}\ 9)$$

Note: See problem 5 for the calculation of the modular inverses.

a) Since an inverse of 19 modulo 141 is 52, i.e., $19 \cdot 52 \equiv 1 (\text{mod } 141)$ and here we want $19x \equiv 4 (\text{mod } 141)$, we can let $x = 4 \cdot 52 = 208$. Since $208 = 67 (\text{mod } 141)$, so $x = 67$ is the smallest positive integer that satisfies the modulo congruence.

b) Since an inverse of 55 modulo 89 is 34, i.e., $55 \cdot 34 \equiv 1 (\text{mod } 89)$ and here we want $55x \equiv 34 (\text{mod } 89)$, we can let $x = 34 \cdot 34 = 1156$. Since $1156 = 88 (\text{mod } 89)$, so $x = 88$ the smallest positive integer that satisfies the modulo congruence.

c) Since an inverse of 89 modulo 232 is 73, i.e., $89 \cdot 73 \equiv 1 (\text{mod } 232)$ and here we want $89x \equiv 2 (\text{mod } 232)$, we can let $x = 2 \cdot 73 = 146$. Since $146 < 232$, $x = 146$ is the smallest positive integer that satisfies the modulo congruence.

EX 22.

. Find the solutions of the congruence $15x^2 + 19x \equiv 5 \pmod{11}$. [*Hint:* Show the congruence is equivalent to the congruence $15x^2 + 19x + 6 \equiv 0 \pmod{11}$. Factor the left-hand side of the congruence; show that a solution of the quadratic congruence is a solution of one of the two different linear congruences.]

$$15x^2 + 19x \equiv 5(mod 11)$$
$$15x^2 + 19x + 6 \equiv 0(mod 11)$$

We factorise the equation and we proceed to solve each part.

$$(3x + 2)(5x + 3) \equiv 0(mod 11)$$
$$\text{So we have two options:}$$

We know that the inverse of 2 mod11 is 9 because 9 + 2 is 11 and 11/11 has a remainder of cero.

We add this inverse on both sides. Then we calcultate the inverse of 3 mod 11

$$\text{Working on option one:}$$
$$3x + 2 \equiv 0(mod 11)$$
$$3x + 2 + 9 \equiv 9(mod 11)$$
$$3x \equiv 9mod(11)$$

We use Bezout's Theorem and the algorithm for division and find out that the inverse is 4.

We multiply each side by 4.

$$11 = (3 * 3) + 2$$
$$3 = (1 * 2) + 1$$
Then...
$$1 = 3 - 2$$
$$1 = 3 - (11 - 3 * 3)$$
$$1 = (3 * 4) - 11$$

So...
$$4 * 3x \equiv 4 * 9(mod 11)$$
$$x \equiv 36(mod 11)$$
$$x \equiv 3(mod 11)$$

We work similarly but now we have to find out the inverse of 5 mod11

Working on option two:
$$5x + 3 \equiv 0(mod 11)$$
$$5x + 3 + 8 \equiv 8(mod 11)$$
$$5x \equiv 8mod(11)$$

We use Bezout's Theorem and the algorithm for division and find out that the inverse is -2; that is also 9.

We multiply each side by 4.

$$11 = (2 * 5) + 1$$
Then...
$$1 = 11 - 2 * 5$$
$$1 = 11 + (-2) * 5$$

So...
$$9 * 5x \equiv 9 * 8(mod 11)$$
$$x \equiv 72(mod 11)$$
$$x \equiv 6(mod 11)$$

We now have the system solved.
$$\{3, 6\}$$

a) Show that $2^{340} \equiv 1 \pmod{11}$ by Fermat's little theorem and noting that $2^{340} = (2^{10})^{34}$.

b) Show that $2^{340} \equiv 1 \pmod{31}$ using the fact that $2^{340} = (2^5)^{68} = 32^{68}$.

c) Conclude from parts (a) and (b) that $2^{340} \equiv 1 \pmod{341}$.

By Fermat's Little Theorem, $2^{10} \equiv 1 \, (mod \, 11)$. So, raising it to the power 34, we obtain $(2^{10})^{34} \equiv 1^{34} \equiv 1 \, (mod \, 11)$

a) $2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \, (mod \, 11)$

Since $32 \equiv 1 \, (mod \, 31)$, thus, $32^{68} \equiv (2^5)^{68} \equiv 1^{68} \equiv 1 \, (mod \, 31)$

b) $2^{340} \equiv (2^5)^{68} \equiv 32^{68} \equiv 1^{68} \equiv 1 \, (mod \, 31)$

$11 \mid (2^{340}-1) \Rightarrow (2^{340}-1) = 11p$ where $gcd(11,p) = 1 \ldots (i)$
$31 \mid (2^{340}-1) \Rightarrow (2^{340}-1) = 31q$ where $gcd(31,q) = 1 \ldots (ii)$
So, from (i) and (ii)
$11p = 31q \Rightarrow 31 \mid 11p$. Since, $gcd(31,11) = 1 \Rightarrow 31 \mid p \Rightarrow p = 31q_1 \ldots (iii)$.
Using (iii) in (i), $(2^{340}-1) = 1p = 11*31q_1 = 341q_1$

$\therefore 341 \mid (2^{340}-1)$

c) $2^{340} \equiv 1 \,(mod\ 11) \Rightarrow 11 \mid (2^{340}-1)$
$2^{340} \equiv 1 \,(mod\ 31) \Rightarrow 31 \mid (2^{340}-1)$
$\therefore 341 \mid (2^{340}-1)$

Hence, $2^{340} \equiv 1 \,(mod\ 341)$