Sabbir Ahmed

DATE: March 6, 2018

MATH 407: HW 04

1.3 **1** Solve the following congruence

d $19x \equiv 1 \pmod{36}$

Ans

$$
\begin{aligned}
19x &\equiv 1 \pmod{36} \\
19x &= 1 + 36n, \text{ for } n \in \mathbb{Z} \\
\Rightarrow 1 &= 19x - 36n \\
1 &= 19(19) - 36(10)
\end{aligned}
$$

Therefore, $x \equiv 19 \pmod{36}$ □

4 Solve the following congruence: $20x \equiv 12 \pmod{72}$

Ans Since $(20, 72) = 4$, there exists 4 solutions.

$$
\begin{aligned}
20x &\equiv 12 \pmod{72} \\
20x &= 12 + 72n, \text{ for } n \in \mathbb{Z} \\
\Rightarrow 5x &= 3 + 18n \\
5x &\equiv 3 \pmod{18}
\end{aligned}
$$

Then, $x \equiv 15 \pmod{18} \Rightarrow 18 \mid (5x - 3)$

Therefore,

$$
\begin{aligned}
x &\equiv 15 \pmod{18} \\
x &\equiv 33 \pmod{18} \\
x &\equiv 51 \pmod{18} \\
x &\equiv 69 \pmod{18}
\end{aligned}
$$

□

7 The smallest positive solution of the congruence $ax \equiv 0 \pmod{n}$ is called the additive order of a modulo n. Find the additive orders of each of the following elements, by solving the appropriate congruences.

b 7 modulo 12

Ans The smallest positive solution: $7x \equiv 0 \pmod{12}$

That is, the smallest positive integer x such that $12 \mid 7x \Rightarrow x = 4$

Therefore, the additive order of 7 modulo 12 is $x = 12$ □

d 12 modulo 18

Ans The smallest positive solution: $12x \equiv 0 \pmod{18}$

That is, the smallest positive integer x such that $18 \mid 12x \Rightarrow x = 3$

Therefore, the additive order of 12 modulo 18 is $x = 3$ □

14 Find the units digit of $3^{29} + 11^{12} + 15$.

Hint: Choose an appropriate modulus n, and then reduce modulo n.

Ans Since $3^4 = 81$ with a units digit of 1,

then $3^{29} = (3^4)^7 \cdot 3$ with a units digit of 3

Since $11^2 = 121$ with a units digit of 1,

then $11^{12} = (11^2)^6$ with a units digit of 1

Therefore, the units digit of $3^{29} + 11^{12} + 15$ is: $1 + 3 + 5 = 9$ □

16 Solve the following congruences by trial and error.

a $x^3 + 2x + 2 \equiv 0 \pmod 5$

Ans By trial and error

$$x = 1 \Rightarrow 5 \mid (1)^3 + 2(1) + 2 = 5$$
$$x = 2 \Rightarrow 5 \nmid (2)^3 + 2(2) + 2 = 14$$
$$x = 3 \Rightarrow 5 \mid (3)^3 + 2(3) + 2 = 35$$
$$x = 4 \Rightarrow 5 \nmid (4)^3 + 2(4) + 2 = 74$$

Therefore,

$x \equiv 1 \pmod 5$ and $x \equiv 3 \pmod 5$ □

20 Solve the following system of congruences.

$$2x \equiv 5 \pmod 7 \qquad\qquad 3x \equiv 4 \pmod 8$$

Ans Simplifying the congruences first,

$2x \equiv 5 \pmod 7$

$$\begin{aligned}
2x &\equiv 5 \pmod 7 \\
2v &\equiv 1 \pmod 7 \\
2v &= 1 - 7n, \text{ for } n \in \mathbb{Z} \\
\Rightarrow 1 &= 2v + 7n \\
1 &= 2(4) + 7(-1) \\
\Rightarrow x &\equiv 4v \pmod 7
\end{aligned}$$

Therefore,

$$\begin{aligned}
2x &\equiv 4 \cdot 5 \pmod 7 \\
x &\equiv 6 \pmod 7
\end{aligned}$$

And $3x \equiv 4 \pmod 8$

$$\begin{aligned}
3x &\equiv 4 \pmod 8 \\
3v &\equiv 1 \pmod 8 \\
3v &= 1 - 8n, \text{ for } n \in \mathbb{Z} \\
\Rightarrow 1 &= 3v + 8n \\
1 &= 3(3) + 8(-1) \\
\Rightarrow x &\equiv 3v \pmod 8
\end{aligned}$$

Therefore,

$$\begin{aligned}
3x &\equiv 3 \cdot 4 \pmod 8 \\
x &\equiv 4 \pmod 8
\end{aligned}$$

Now the system can be solved using the Chinese Remainder Theorem:

$$x \equiv 6 \pmod 7 \qquad\qquad x \equiv 4 \pmod 8$$

Since $(n_1, n_2) = (7, 8) = 1$, let $u_1 = 7k_1$ and $u_2 = 8k_2$

Then

$$u_1 + u_2 = 1 \Rightarrow 7k_1 + 8k_2 = 1$$
$$1 = 7(-1) + 8(1)$$

Thus

$$u_1 = 7(-1) = -7 \equiv 1 \pmod{8}$$
$$u_1 = 7(-1) = -7 \equiv 0 \pmod{7}$$

And

$$u_2 = 8(1) = 8 \equiv 0 \pmod{8}$$
$$u_2 = 8(1) = 8 \equiv 1 \pmod{7}$$

Therefore,

$$\begin{aligned} x &= 6u_1 + 4u_2 \\ &= 6(-7) + 4(8) \\ &= -10 \end{aligned}$$

Therefore, the general solution with the smallest nonnegative integer is

$$x \equiv -10 \pmod{n_1 n_2}$$
$$x \equiv -10 \pmod{56}$$
$$x \equiv 46 \pmod{56}$$

□

1.4 **2** Make multiplication tables for the following sets.

□

□

Table 1: b: Multiplication table of $\mathbb{Z}_7$

$\times$	$[\mathbf{0}]$	$[\mathbf{1}]$	$[\mathbf{2}]$	$[\mathbf{3}]$	$[\mathbf{4}]$	$[\mathbf{5}]$	$[\mathbf{6}]$
$[\mathbf{0}]$	[0]	[0]	[0]	[0]	[0]	[0]	[0]
$[\mathbf{1}]$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
$[\mathbf{2}]$	[0]	[2]	[4]	[6]	[1]	[3]	[5]
$[\mathbf{3}]$	[0]	[3]	[6]	[2]	[5]	[1]	[4]
$[\mathbf{4}]$	[0]	[4]	[1]	[5]	[2]	[6]	[3]
$[\mathbf{5}]$	[0]	[5]	[3]	[1]	[6]	[4]	[2]
$[\mathbf{6}]$	[0]	[6]	[5]	[4]	[3]	[2]	[1]

Table 2: c: Multiplication table of $\mathbb{Z}_8$

$\times$	$[\mathbf{0}]$	$[\mathbf{1}]$	$[\mathbf{2}]$	$[\mathbf{3}]$	$[\mathbf{4}]$	$[\mathbf{5}]$	$[\mathbf{6}]$	$[\mathbf{7}]$
$[\mathbf{0}]$	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
$[\mathbf{1}]$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
$[\mathbf{2}]$	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
$[\mathbf{3}]$	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
$[\mathbf{4}]$	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
$[\mathbf{5}]$	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
$[\mathbf{6}]$	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
$[\mathbf{7}]$	[0]	[7]	[5]	[4]	[3]	[2]	[1]	[1]

6 Let m and n be positive integers such that $m \mid n$. Show that for any integer a, the congruence class $[a]_m$ is the union of the congruence classes $[a]_n, [a+m]_n, [a+2m]_n, \ldots, [a+n-m]_n$

Ans To show

$$[a]_m = [a]_n \cup [a+m]_n \cup [a+2m]_n \cup \ldots \cup [a+n-m]_n$$

Let $x \in [a+km]_n$, for $k \in \mathbb{Z}$

Then $x \equiv a + km \pmod{n}$

$\Rightarrow x = a + km + ln$, for $l \in \mathbb{Z}$

Since $m \mid n$,

$n = pm$, for $p \in \mathbb{Z}$

Then

$$\begin{aligned} x &= a + km + l(pm) \\ &= a + (k + lp)m \\ \Rightarrow x &\equiv a \pmod{m} \\ \Rightarrow x &\in [a]_m \end{aligned}$$

Thus

$$[a]_n \cup [a+m]_n \cup [a+2m]_n \cup \ldots \cup [a+n-m]_n \subseteq [a]_m$$

Conversely,

Let $x \in [a]_m$

Then,

$$\begin{aligned} x &\equiv a \pmod{m} \\ \Rightarrow x &= a + lm, \text{ for } l = k + n \\ &= a + (k+n)m \\ &= a + km + mn \\ \Rightarrow x &\equiv km \pmod{n} \\ \Rightarrow x &\in [a+km]_n \end{aligned}$$

Thus

$$[a]_m \subseteq [a]_n \cup [a+m]_n \cup [a+2m]_n \cup \ldots \cup [a+n-m]_n$$

$\therefore [a]_m = [a]_n \cup [a+m]_n \cup [a+2m]_n \cup \ldots \cup [a+n-m]_n$ $\square$

9 Let $gcd(a, n) = 1$. The smallest positive integer k such that $a^k \equiv 1 \pmod{n}$ is called the **multiplicative order** of $[a]$ in $\mathbb{Z}_n^\times$

b Find the multiplicative orders of $[2]$ and $[5]$ in $\mathbb{Z}_{17}^\times$.

Ans Show $2^k \equiv 1 \pmod{17}$, for $k \in \mathbb{Z}$

Then, $2^k = 1 + 17n$, for $n \in \mathbb{Z}$

Then, $n = (2^k - 1)/17$

Therefore, for n to be an integer, $k = 8$.

Similarly, show $5^k \equiv 1 \pmod{17}$, for $k \in \mathbb{Z}$

Then, $5^k = 1 + 17n$, for $n \in \mathbb{Z}$

Then, $n = (5^k - 1)/17$

Therefore, for n to be an integer, $k = 16$.

Therefore, the multiplicative order of $[2]$ and $[5]$ in $\mathbb{Z}_{17}^\times$ is $k = 8$ □

10 Let $gcd(a, n) = 1$. If $[a]$ has multiplicative order k in $\mathbb{Z}_n^\times$, show that $k \mid \varphi(n)$.

Ans By Euler's theorem, if $gcd(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$

Also, if k is the multiplicative order of $[a]$,

then k is the smallest positive interger such that $a^k \equiv 1 \pmod{n}$

Therefore, there exists an $m \in \mathbb{Z}$ such that

$$a^{mk} = a^{\varphi(n)} \equiv 1 \pmod{n}$$

Then $mk = \varphi(n)$

That is, $k \mid \varphi(n)$ □

13 An element $[a]$ of is said to be **idempotent** if $[a]^2 = [a]$.

b Find all idempotent elements of $\mathbb{Z}_{10}^\times$ and $\mathbb{Z}_{30}^\times$.

Ans For $\mathbb{Z}_{10}^\times$:

$$[0]^2 = [0]$$

$$[1]^2 = [1]$$

$$[5]^2 = [5]$$

$$[6]^2 = [6]$$

For $\mathbb{Z}_{30}^{\times}$:

$$[0]^2 = [0]$$
$$[1]^2 = [1]$$
$$[6]^2 = [6]$$
$$[10]^2 = [10]$$

□

15 If n is not a prime power, show that $\mathbb{Z}_n$ has an idempotent element different from $[0]$ and $[1]$.

Hint: Suppose that $n = bc$, with $gcd(b, c) = 1$. Solve the simultaneous congruences $x \equiv 1 \pmod b$ and $x \equiv 0 \pmod c$.

Ans Let $n = bc$, with $gcd(b, c) = 1$

Since $gcd(b, c)$, the Chinese remainder theorem may be applied to the congruences:

$$x \equiv 1 \pmod b \qquad\qquad x \equiv 0 \pmod c$$

Consider

$x - 1 \equiv 0 \pmod b$ and $x \equiv 0 \pmod c$

That is

$$x(x-1) \equiv 0 \pmod{bc}$$
$$x^2 - x \equiv 0 \pmod{bc}$$
$$x^2 \equiv x \pmod{bc}$$
$$x^2 \equiv x \pmod n$$

Therefore, there exists an idempotent element in $\mathbb{Z}_n$ different from $[0]$ and $[1]$ □

20 Show that $\varphi(1) + \varphi(p) + \ldots + \varphi(p^\alpha) = p^\alpha$ for any prime number p and any positive integer α.

Ans Since

$$\begin{aligned}\varphi(p^\alpha) &= p^\alpha\left(1 - \frac{1}{p}\right)\\ &= p^\alpha - p\\ &= p^{\alpha-1}(p-1)\end{aligned}$$

Then

$$\begin{aligned}\varphi(1)+\varphi(p)+\varphi(p^2)+\ldots+\varphi(p^\alpha) &= (p^{-1}(p-1)) + (p^0(p-1)) + (p^1(p-1)) + \ldots + p^{\alpha-1}(p-1)\\ &= 1+p-1+p^2-p\ldots+p^\alpha-p^{\alpha-1}\\ &= p^\alpha \qquad \square\end{aligned}$$

26 Let $p = 2k+1$ be a prime number. Show that if a is an integer such that $p \nmid a$, then either $a^k \equiv 1 \pmod p$ or $a^k \equiv -1 \pmod p$

Ans Using Fermat's little theorem:
If p is prime and $p \nmid a$, then

$$\begin{aligned}a^{p-1} &\equiv 1 \pmod p\\ a^{(2k+1)-1} &\equiv 1 \pmod{(2k+1)}\\ a^{2k} &\equiv 1 \pmod{(2k+1)}\\ (a^k)^2 &\equiv 1 \pmod{(2k+1)}\end{aligned}$$

Therefore,

$$a^k \equiv \pm 1 \pmod p$$

$$\therefore a^k \equiv 1 \pmod p \text{ or } a^k \equiv -1 \pmod p \qquad \square$$