Discrete Mathematics
Week 8

Abeyah Calpatura

8.3

Exercises

Abeyah Calpatura
#3,7, 15ab, 16a, 17,36, 37, 38

#3 Solution:

$$A = \{0, 1, 2, 3, 4\}$$
$$R = \{(0,0), (0,4), (1,1), (1,3), (2,2), (3,1), (3,3), (4,0), (4,4)\}$$

equivalence classes: [0], [1], [2], [3]

$[0] = \{x \in A \mid x\, R\, 0\} = \{0, 4\}$
$[1] = \{x \in A \mid x\, R\, 1\} = \{1, 3\}$
$[2] = \{x \in A \mid x\, R\, 2\} = \{2\}$
$[3] = \{x \in A \mid x\, R\, 3\} = \{1, 3\}$
$[4] = \{x \in A \mid x\, R\, 4\} = \{0, 4\}$

The distinct equivalence classes of the relation R are $\{0, 4\}, \{2\}, \{1, 3\}$

#7 Solution: $A = \{(1,3), (2,4), (-4,-8), (3,9), (1,5), (3,6)\}$
R is defined on A as follows: For every (a, b), (c, d) $\in A$,

$$(a, b)\, R\, (c, d) \iff ad = bc$$

Find the distinct equivalence classes of the relation R.

$[(1,3)] = \{(a,b) \in A : (a,b)R(1,3)\}$
$= \{(a,b) \in A : 3a = b\}$
$= \{(1,3), (3,9)\}$

$[(2,4)] = \{(a,b) \in A : (a,b)R(2,4)\}$
$= \{(a,b) \in A : 4a = 2b\}$
$= \{(2,4), (-4,-8), (3,6)\}$

$[(1,5)] = \{(a,b) \in A : (a,b)R(1,5)\}$
$= \{(a,b) \in A : 5a = b\}$
$= \{(1,5)\}$

#15a ***Solution:*** $17 \equiv 2 \pmod 5$

$$17 - 2 = 15 = 3 \cdot 5$$
True

#15b ***Solution:*** $4 \equiv -5 \pmod 7$
s

$$4 - (-5) = 4 + 5 = 9$$
False

#16a ***Solution:*** Let R be the relation of congruence modulo 3. Which of the following equivalence classes are equal?

$$[7], [-4], [-6], [17], [4], [27], [19]$$

$$R = \text{Relation of congruence modulo 3}$$

Equivalence class	a - 7	3 divides a - 7	Equal to equivalence class [7]
[-4]	$-4 - 7 = -11$	No	No
[-6]	$-6 - 7 = -13$	No	No
[17]	$17 - 7 = 10$	No	No
[4]	$4 - 7 = -3$	Yes	Yes
[27]	$27 - 7 = 20$	No	No
[19]	$19 - 7 = 12$	Yes	Yes

Implies: [7] = [4] = [19]

Equivalence class	$a - (-4)$	3 divides $a - (-4)$	Equal to equivalence class [-4]
[-6]	$-6 - (-4) = -2$	No	No
[17]	$17 - (-4) = 21$	Yes	Yes
[27]	$27 - (-4) = 31$	No	No

Implies: $[-4] = [17]$

Equivalence class	$a - (-6)$	3 divides $a - (-6)$	Equal to equivalence class [-6]
[27]	$27 - (-6) = -33$	Yes	Yes

Implies: $[-6] = [27]$

s**#17a** ***Solution:*** Prove that all integers m and n, $m \equiv n \pmod 3$ if, and only if *m mod 3 = n mod 3*

Let m and n be integers
Let m mod 3 = n mod 3
Then, m = 3a + b and n = 3c + b, where a, b, c are integers and $0 \leqslant b < 3$
Then, m - n = 3a + b - 3c - b
m - n = 3(a - c)
3 divides m - n
$m \equiv n \pmod 3$

#17b *Solution:* Prove that for all integers m and n and any positive integer d, $m \equiv n \pmod{d}$ if, and only if, $m \; mod \; d = n \; mod \; d$

Let m and n be integers

Let m mod d = n mod d

Then, m = da + b and n = dc + b, where a, b, c are integers and $0 \leqslant b < d$

Then, m - n = da + b - dc - b

m - n = d(a - c)

d divides m - n

$m \equiv n \pmod{d}$

#36 *Solution:* For every a in A, $a \in A$

Let $a \in A$

Since R is an equivalence relation, R is reflexive, symmetric, and transitive

By definition of reflexive: (a, a) $\in R$ or equivalently a R a

a R a is true and since $a \in A$, we note that $a \in [a]$

#37 *Solution:* For every a and b in A, if $b \in [a]$ then $a \; R \; b$.

Let a and b be in A

Let $b \in [a]$

By definition of equivalence class: $b \in [a]$ if and only if $b \in A$ and $a \; R \; b$

Since $b \in [a]$, $b \in A$ and $a \; R \; b$

Therefore, if $b \in [a]$ then $a \; R \; b$ by using that R is symmetric and definition of the equivalence class

#38 *Solution:* For every a, b, and c in A, if $b \; R \; c$ and $c \in [a]$ then $b \in [a]$.

Let a, b, and c be in A

Let $b \; R \; c$ and $c \in [a]$

By definition of equivalence class: $c \in [a]$ if and only if $c \in A$ and $a \; R \; c$

Since $c \in [a]$, $c \in A$ and $a \; R \; c$

Since $b \; R \; c$, $b \; R \; c$ and $a \; R \; c$

Prove using that R is transitive and the definitino of equivalence class

8.4

Exercises

Abeyah Calpatura
#1, 3, 7, 14, 15,19, 22, 26, 31, 36, 39

#1a ***Solution:*** WHERE SHALL WE MEET

$$23\ 08\ 05\ 18\ 05\ 19\ 08\ 01\ 12\ 12\ 23\ 05\ 13\ 05\ 05\ 20$$
$$C = (M + 3)$$
$$26\ 11\ 08\ 21\ 08\ 22\ 11\ 04\ 15\ 15\ 26\ 08\ 16\ 08\ 08\ 23$$
$$\text{ZKHUH VKDOO ZH PHHW}$$

#1b ***Solution:*** LQ WKH FDIHWHULD

$$12\ 17\ 23\ 11\ 08\ 06\ 04\ 09\ 08\ 23\ 08\ 21\ 12\ 04$$
$$C = (M - 3)$$
$$09\ 14\ 20\ 20\ 08\ 05\ 03\ 01\ 06\ 05\ 20\ 05\ 18\ 09\ 01$$
$$\text{IN THE CAFETERIA}$$

#3 Let a = 25, b = 19, and n = 3
#3a ***Solution:*** Verify that $3 \mid (25 - 19)$

$$25 - 19 = 6 = 3 \cdot 2$$

#3b ***Solution:*** Explain why $25 \equiv 19 \pmod 3$

Through part a, we determined that 3 divides $25 - 19$

#3c ***Solution:*** What value of k has the proprety that $25 = 19 + 3k$?

$$25 = 19 + 3k$$
$$6 = 3k$$
$$k = 2$$

#3d ***Solution:*** What is the (nonnegative) remainder when 25 is divided by 3? When 19 is divided by 3?

$$25 \div 3 = 8 \text{ remainder } 1$$
$$19 \div 3 = 6 \text{ remainder } 1$$

#3e ***Solution:*** Explain why 25 mod 3 = 19 mod 3

The remainder when 25 is divided by 3 is 1
The remainder when 19 is divided by 3 is 1
Both remainders are 1

#7a ***Solution:*** $128 \equiv 2 \pmod 7$ and $61 \equiv 5 \pmod 7$

$$7 \mid (128 - 2)$$
$$128 - 2 = 126 = 7 \cdot 18$$
$$7 \mid (61 - 5)$$
$$61 - 5 = 56 = 7 \cdot 8$$

#7b ***Solution:*** $(128+61) \equiv (2+5) \pmod 7$

$$
\begin{aligned}
&128+61 = 189\\
&2+5 = 7\\
&7 \mid ((128+61)-(2+5))\\
&7 \mid (189-7)\\
&7 \mid 182\\
&182 = 7 \cdot 26
\end{aligned}
$$

#7c ***Solution:*** $(128-61) \equiv (2-5) \pmod 7$

$$
\begin{aligned}
&128-61 = 67\\
&2-5 = -3\\
&7 \mid ((128-61)-(2-5))\\
&7 \mid (67+3)\\
&7 \mid 70\\
&70 = 7 \cdot 10
\end{aligned}
$$

#7d ***Solution:*** $(128 \cdot 61) \equiv (2 \cdot 5) \pmod 7$

$$
\begin{aligned}
&128 \cdot 61 = 7808\\
&2 \cdot 5 = 10\\
&7 \mid ((128 \cdot 61)-(2 \cdot 5))\\
&7 \mid (7808-10)\\
&7 \mid 7798\\
&7798 = 7 \cdot 1114
\end{aligned}
$$

#7e ***Solution:*** $128^2 \equiv 2^2 \pmod 7$

$$
\begin{aligned}
&128^2 = 16384\\
&2^2 = 4\\
&7 \mid (16384-4)\\
&7 \mid 16380\\
&16380 = 7 \cdot 2340
\end{aligned}
$$

#14 ***Solution:*** Use the technique of Example 8.4.4 to find $14^2\, mod\, 55$, $14^4\, mod\, 55$, $14^8\, mod\, 55$, $14^{16}\, mod\, 55$

$$
\begin{aligned}
&14^2\, mod\, 55 = 196\, mod\, 55 = 31\\
&14^4\, mod\, 55 = (14^2\, mod\, 55)^2 = (31)^2\, mod\, 55 = 26\\
&14^8\, mod\, 55 = (14^4\, mod\, 55)^2 = (26)^2\, mod\, 55 = 16\\
&14^{16}\, mod\, 55 = (14^8\, mod\, 55)^2 = (16)^2\, mod\, 55 = 36
\end{aligned}
$$

#15 ***Solution:*** Use the result of #14 to find $14^{27}\, mod\, 55$

$$
\begin{aligned}
&14^{27}\, mod\, 55 = (14^{16} \cdot 14^8 \cdot 14^2 \cdot 14^1)\, mod\, 55\\
&14^{27}\, mod\, 55 = (31 \cdot 16 \cdot 26 \cdot 36)\, mod\, 55\\
&14^{27}\, mod\, 55 = 249984\, mod\, 55 = 9
\end{aligned}
$$

#19 *Solution:* HELLO

$$
\begin{aligned}
&C = M^e\ mod\ pq\ \ e = 3 \text{ and } pq = 55\\
&\text{08 05 12 12 15}\\
&C = 08^3\ mod 55\ = 512\ mod\ 55 = 17\\
&C = 05^3\ mod 55\ = 125\ mod\ 55 = 15\\
&C = 12^3\ mod 55\ = 1728\ mod\ 55 = 23\\
&C = 12^3\ mod 55\ = 1728\ mod\ 55 = 23\\
&C = 15^3\ mod 55\ = 3375\ mod\ 55 = 20\\
&\text{17 15 23 23 20} = \text{QOWWT}
\end{aligned}
$$

#22 *Solution:* 13 20 20 09

$$
\begin{aligned}
&M = C^d modpq \text{ with } d = 27 \text{ and } pq = 55\\
&C = 13^{27}\ mod\ 55 = 7\\
&C = 20^{27}\ mod\ 55 = 15\\
&C = 20^{27}\ mod\ 55 = 15\\
&C = 09^{27}\ mod\ 55 = 4\\
&\text{07 15 15 04} = \text{GOOD}
\end{aligned}
$$

#26 *Solution:* Use Euclidean algorith to find greatest common divisor of 6664 and 765. Express as linear combination of two numbers.

$$
\begin{aligned}
&6664 = 8 \cdot 765 + 544\\
&765 = 1 \cdot 544 + 221\\
&554 = 2 \cdot 221 + 102\\
&221 = 2 \cdot 102 + 17\\
&102 = 6 \cdot 17 + 0\\
&\gcd(6664,\ 765) = 17\\
&17 = 221 - 2 \cdot 102\\
&17 = 221 - 2(544 - 2(221))\\
&17 = 5(221) - 2(544)\\
&17 = 5(765 - 544) - 2(544)\\
&17 = 5(765) - 7(544)\\
&17 = 5(765) - 7(6664 - 8(765))\\
&17 = 61 \cdot 765 - 7 \cdot 6664
\end{aligned}
$$

#31a ***Solution:*** Find an inverse for 210 modulo 13

$$\begin{aligned}
&210 = 16 \cdot 13 + 2\\
&13 = 6 \cdot 2 + 1\\
&2 = 2 \cdot 1 + 0\\
&\gcd(210,\ 13) = 1\\
&1 = 13 - 6 \cdot 2\\
&1 = 13 - 6(210 - 16 \cdot 13)\\
&1 = 97 \cdot 13 - 6 \cdot 210\\
&((-6) \cdot 210)\ mod\ 13 = (1 - 97 \cdot 13)\ mod\ 13\\
&((-6) \cdot 210)\ mod\ 13 = 1
\end{aligned}$$

Therefore, the inverse of 210 modulo 13 is -6

#31b ***Solution:*** Find a positive inverse for 210 modulo 13

$$\begin{aligned}
&-6\ mod\ 13 = (-6 + 0)\ mod\ 13\\
&(-6\ mod\ 13 + 13\ mod\ 13)\ mod\ 13\ ;\ //\ 0\ mod\ 13 = 0 = 13\\
&(-6 + 13)\ mod\ 13\\
&7\ mod\ 13
\end{aligned}$$

Therefore, the positive inverse of 210 modulo 13 is 7

#31c ***Solution:*** Find a positive solution for the congruence $210x \equiv 8 \pmod{13}$

$a \equiv b \pmod{c}$ is equivalent with $a\ mod\ c = b\ mod\ c$

$$\begin{aligned}
&210x \equiv 8 \pmod{13}\\
&210x\ mod\ 13 = 8\ mod\ 13\\
&x\ mod\ 13 = 7 \cdot 8\ mod\ 13\\
&x\ mod\ 13 = 56\ mod\ 13\\
&x\ mod\ 13 = 4
\end{aligned}$$

Therefore, the positive solution for the congruence $210x \equiv 8 \pmod{13}$ is 4

#36 ***Solution:*** HELP, $n = 713 = 23 \cdot 31$ and $e = 43$

$$\begin{aligned}
&C = M^e\ mod\ pq\\
&\text{H is } 8^43\ mod\ 713 = 233\\
&\text{E is } 5^43\ mod\ 713 = 129\\
&\text{L is } 12^43\ mod\ 713 = 048\\
&\text{P is } 16^43\ mod\ 713 = 128
\end{aligned}$$

#39 Solution: $n = 713 = 23 \cdot 31$ and $e = 43$ and $d = 307$ the inverse of 43 where $d \equiv e^{-1} \pmod{\phi(n)}$ where $n = pq$ and $\phi(n) = (p-1)(q-1)$

$$\begin{aligned}
&675089089048\\
&675^{307}\ mod\ 713 = 3\\
&089^{307}\ mod\ 713 = 15\\
&089^{307}\ mod\ 713 = 15\\
&048^{307}\ mod\ 713 = 12
\end{aligned}$$

The message is COOL