MTH 4441 - HW #4 - Modulo Arithmetic (Solutions)

FALL 2017

Pat Rossi Name ______________________________

1. Compute the congruent values modulo n:

   (a) $(26+35) \equiv$ ____ $\bmod 5$

   $26+35=61$ and 61 leaves a **remainder of 1** when divided by 5

Hence, $(26+35) \equiv 1 \bmod 5$

   Alternatively:

   26 leaves a **remainder of 1** when divided by 5.

   Hence, $26 \bmod 5 \equiv 1$

   Also:

   35 leaves a **remainder of 0** when divided by 5.

   Hence, $35 \bmod 5 \equiv 0$

   Thus, $(26+35) \equiv (1+0) \bmod 5 \equiv 1 \bmod 5$

i.e., $(26+35) \equiv 1 \bmod 5$

   (b) $(84+91) \equiv$ ____ $\bmod 13$

   $84+91=175$ and 175 leaves a **remainder of 6** when divided by 13

Hence, $(84+91) \equiv 6 \bmod 13$

   Alternatively:

   84 leaves a **remainder of 6** when divided by 13.

   Hence, $84 \bmod 13 \equiv 6$

   Also:

   91 leaves a **remainder of 0** when divided by 13.

   Hence, $91 \bmod 13 \equiv 0$

   Thus, $(84+91) \equiv (6+0) \bmod 13 \equiv 6 \bmod 13$

i.e., $(84+91) \equiv 6 \bmod 13$

(c) $(29+57) \equiv$ ____ $\bmod 6$

$29+57=86$ and 86 leaves a **remainder of 2** when divided by 6

Hence, $(29+57) \equiv 2 \bmod 6$

Alternatively:

29 leaves a **remainder of 5** when divided by 6.

Hence, $29 \bmod 6 \equiv 5$

Also:

91 leaves a **remainder of 0** when divided by 13.

Hence, $57 \bmod 6 \equiv 3$

Thus, $(29+57) \equiv (5+3) \bmod 6 \equiv 8 \bmod 6 \equiv 2 \bmod 6$

i.e., $(29+57) \equiv 2 \bmod 6$

(d) $(45+36) \equiv$ ____ $\bmod 12$

$45+36=81$ and 81 leaves a **remainder of 9** when divided by 12

Hence, $(45+36) \equiv 9 \bmod 12$

Alternatively:

45 leaves a **remainder of 9** when divided by 12.

Hence, $45 \bmod 12 \equiv 9$

Also:

36 leaves a **remainder of 0** when divided by 12.

Hence, $36 \bmod 12 \equiv 0$

Thus, $(45+36) \equiv (9+0) \bmod 12 \equiv 9 \bmod 12$

i.e., $(45+36) \equiv 9 \bmod 12$

(e) $(45 + 36) \equiv$ ____ $\bmod 9$

$45 + 36 = 81$ and 81 leaves a **remainder of 0** when divided by 9

Hence, $(45 + 36) \equiv 0 \bmod 9$

Alternatively:

45 leaves a **remainder of 0** when divided by 9.

Hence, $45 \bmod 9 \equiv 0$

Also:

36 leaves a **remainder of 0** when divided by 9.

Hence, $36 \bmod 9 \equiv 0$

Thus, $(45 + 36) \equiv (0 + 0) \bmod 9 \equiv 0 \bmod 9$

i.e., $(45 + 36) \equiv 0 \bmod 9$

2. Compute the congruent values modulo n:

(a) $(26 \cdot 35) \equiv$ ____ $\bmod 5$

$26 \cdot 35 = 910$ and 910 leaves a **remainder of 0** when divided by 5

Hence, $(26 \cdot 35) \equiv 0 \bmod 5$

Alternatively:

26 leaves a **remainder of 1** when divided by 5.

Hence, $26 \bmod 5 \equiv 1$

Also:

35 leaves a **remainder of 0** when divided by 5.

Hence, $35 \bmod 5 \equiv 0$

Thus, $(26 \cdot 35) \equiv (1 \cdot 0) \bmod 5 \equiv 0 \bmod 5$

i.e., $(26 \cdot 35) \equiv 0 \bmod 5$

(b) $(84 \cdot 92) \equiv \_\_\_\_ \bmod 13$

$84 \cdot 92 = 7728$ and 7728 leaves a **remainder of 6** when divided by 13

Hence, $(84 \cdot 92) \equiv 6 \bmod 13$

Alternatively:

84 leaves a **remainder of 6** when divided by 13.

Hence, $84 \bmod 13 \equiv 6$

Also:

92 leaves a **remainder of 1** when divided by 13.

Hence, $92 \bmod 13 \equiv 1$

Thus, $(84 \cdot 92) \equiv (6 \cdot 1) \bmod 13 \equiv 6 \bmod 13$

i.e., $(84 \cdot 92) \equiv 6 \bmod 13$

(c) $(29 \cdot 57) \equiv \_\_\_\_ \bmod 6$

$29 \cdot 57 = 1653$ and 1653 leaves a **remainder of 3** when divided by 6

Hence, $(29 \cdot 57) \equiv 3 \bmod 6$

Alternatively:

29 leaves a **remainder of 5** when divided by 6.

Hence, $29 \bmod 6 \equiv 5$

Also:

57 leaves a **remainder of 3** when divided by 6.

Hence, $57 \bmod 6 \equiv 3$

Thus, $(29 \cdot 57) \equiv (5 \cdot 3) \bmod 6 \equiv 15 \bmod 6 \equiv 3 \bmod 6$

i.e., $(29 \cdot 57) \equiv 3 \bmod 6$

(d) $(45 \cdot 36) \equiv \_\_\_\_ \bmod 12$

$45 \cdot 36 = 1620$ and 1620 leaves a **remainder of 0** when divided by 12

Hence, $(45 \cdot 36) \equiv 0 \bmod 12$

Alternatively:

45 leaves a **remainder of 9** when divided by 12.

Hence, $45 \bmod 12 \equiv 9$

Also:

36 leaves a **remainder of 0** when divided by 12.

Hence, $36 \bmod 12 \equiv 0$

Thus, $(45 \cdot 36) \equiv (9 \cdot 0) \bmod 12 \equiv 0 \bmod 12$

i.e., $(45 \cdot 36) \equiv 0 \bmod 12$

(e) $(45 \cdot 36) \equiv \_\_\_\_ \bmod 8$

$45 \cdot 36 = 1620$ and 1620 leaves a **remainder of 4** when divided by 8

Hence, $(45 \cdot 36) \equiv 4 \bmod 8$

Alternatively:

45 leaves a **remainder of 5** when divided by 8.

Hence, $45 \bmod 8 \equiv 5$

Also:

36 leaves a **remainder of 4** when divided by 8.

Hence, $36 \bmod 8 \equiv 4$

Thus, $(45 \cdot 36) \equiv (5 \cdot 4) \bmod 8 \equiv 20 \bmod 8 \equiv 4 \bmod 8$

i.e., $(45 \cdot 36) \equiv 4 \bmod 8$

(f) $(27 \cdot 36) \equiv$ ____ $\bmod 15$

$27 \cdot 36 = 972$ and 972 leaves a **remainder of 12** when divided by 15

Hence, $(27 \cdot 36) \equiv 12 \bmod 15$

Alternatively:

27 leaves a **remainder of 12** when divided by 15.

Hence, $27 \bmod 15 \equiv 12$

Also:

36 leaves a **remainder of 6** when divided by 15.

Hence, $36 \bmod 15 \equiv 6$

Thus, $(27 \cdot 36) \equiv (12 \cdot 6) \bmod 15 \equiv 72 \bmod 15 \equiv 12 \bmod 15$

i.e., $(27 \cdot 36) \equiv 12 \bmod 15$

3. Express the following integers as a "proper remainder" modulo n.

(a) $26 \equiv$ ____ $\bmod 7$

$26 = (3)(7) + 5$ (i.e., 26 leaves a "proper remainder" of 5 when divided by 7)

Hence, $26 \equiv 5 \bmod 7$

Alternatively:

Since integers that are congruent to one another mod 7 are exactly those integers that differ from one another by a whole number multiple of 7, we can successively add or subtract multiples of **7**, until we get a number between 0 and 6 (i.e., until we get a number between 0 and $(7 - 1)$)

$26 \equiv 19 \bmod 7 \equiv 12 \bmod 7 \equiv 5 \bmod 7$

Hence, $26 \equiv 5 \bmod 7$

(b) $-32 \equiv \_\_\_\_ \bmod 5$

$-32 = (-7)(5) + 3$ (i.e., -32 leaves a "proper remainder" of 3 when divided by 5)

Hence, $-32 \equiv 3 \bmod 5$

Alternatively:

Since integers that are congruent to one another mod 5 are exactly those integers that differ from one another by a whole number multiple of 5, we can successively add or subtract multiples of **5**, until we get a number between 0 and 4 (i.e., until we get a number between 0 and $(5-1)$)

$-32 \equiv -27 \bmod 5 \equiv -22 \bmod 5 \equiv -17 \bmod 5 \equiv -12 \bmod 5 \equiv -7 \bmod 5 \equiv -2 \bmod 5 \equiv 3 \bmod 5$

Hence, $-32 \equiv 3 \bmod 5$

(c) $-29 \equiv \_\_\_\_ \bmod 7$

$-29 = (-5)(7) + 6$ (i.e., -29 leaves a "proper remainder" of 6 when divided by 7)

Hence, $-29 \equiv 6 \bmod 7$

Alternatively:

Since integers that are congruent to one another mod 7 are exactly those integers that differ from one another by a whole number multiple of 7, we can successively add or subtract multiples of **7**, until we get a number between 0 and 6 (i.e., until we get a number between 0 and $(7-1)$)

$-29 \equiv -22 \bmod 7 \equiv -15 \bmod 7 \equiv -8 \bmod 7 \equiv -1 \bmod 7 \equiv 6 \bmod 7$

Hence, $-29 \equiv 6 \bmod 7$

(d) $15 \equiv \_\_\_\_ \bmod 8$

$15 = (1)(8) + 7$ (i.e., 15 leaves a "proper remainder" of 7 when divided by 8)

Hence, $15 \equiv 7 \bmod 8$

Alternatively:

Since integers that are congruent to one another mod 8 are exactly those integers that differ from one another by a whole number multiple of 8, we can successively add or subtract multiples of **8**, until we get a number between 0 and 7 (i.e., until we get a number between 0 and $(8-1)$)

$15 \equiv 7 \bmod 8$

Hence, $15 \equiv 7 \bmod 8$

(e) $-15 \equiv$ ____ $\bmod 8$

$-15 = (-2)(8) + 1$ (i.e., -15 leaves a "proper remainder" of 1 when divided by 8)

Hence, $-15 \equiv 1 \bmod 8$

Alternatively:

Since integers that are congruent to one another mod 8 are exactly those integers that differ from one another by a whole number multiple of 8, we can successively add or subtract multiples of **8**, until we get a number between 0 and 7 (i.e., until we get a number between 0 and $(8-1)$)

$-15 \equiv -7 \bmod 8 \equiv 1 \bmod 8$

Hence, $-15 \equiv 1 \bmod 8$

(f) $-25 \equiv$ ____ $\bmod 8$

$-25 = (-4)(8) + 7$ (i.e., -25 leaves a "proper remainder" of 7 when divided by 8)

Hence, $-25 \equiv 7 \bmod 8$

Alternatively:

Since integers that are congruent to one another mod 8 are exactly those integers that differ from one another by a whole number multiple of 8, we can successively add or subtract multiples of **8**, until we get a number between 0 and 7 (i.e., until we get a number between 0 and $(8-1)$)

$-25 \equiv -17 \bmod 8 \equiv -9 \bmod 8 \equiv -1 \bmod 8 \equiv -7 \bmod 8$

Hence, $-25 \equiv 7 \bmod 8$

(g) $23 \equiv$ ____ $\bmod 8$

$23 = (2)(8) + 7$ (i.e., 23 leaves a "proper remainder" of 7 when divided by 8)

Hence, $23 \equiv 7 \bmod 8$

Alternatively:

Since integers that are congruent to one another mod 8 are exactly those integers that differ from one another by a whole number multiple of 8, we can successively add or subtract multiples of **8**, until we get a number between 0 and 7 (i.e., until we get a number between 0 and $(8-1)$)

$23 \equiv 15 \bmod 8 \equiv 7 \bmod 8$

Hence, $23 \equiv 7 \bmod 8$

4. Compute the congruent values modulo n:

(a) $26^{10} \equiv$ ____ $\bmod 5$

$26^{10} = 141167095653376$ and 141167095653376 leaves a **remainder of 1** when divided by 5

Hence, $26^{10} \equiv 1 \bmod 5$

Alternatively:

26 leaves a **remainder of 1** when divided by 5. Therefore, $26 \equiv 1 \bmod 5$

Hence, $26^{10} \equiv (1)^{10} \bmod 5 \equiv 1 \bmod 5$

i.e., $26^{10} \equiv 1 \bmod 5$

(b) $26^{10} \equiv$ ____ $\bmod 12$

This number is probably too large to deal with directly. So we replace 26 with its equivalent value mod 12.

26 leaves a **remainder of 2** when divided by 12. Therefore, $26 \equiv 2 \bmod 12$

Hence, $26^{10} \equiv 2^{10} \bmod 12 \equiv 1024 \bmod 12 \equiv 4$ (because 1024 leaves a remainder of 4, when divided by 12)

i.e., $26^{10} \equiv 4 \bmod 12$

(c) $45^{14} \equiv$ ____ $\bmod 7$

This number is probably too large to deal with directly. So we replace 45 with its equivalent value mod 7.

45 leaves a **remainder of 3** when divided by 7. Therefore, $45 \equiv 3 \bmod 7$

Hence, $45^{14} \equiv 3^{14} \bmod 7 \equiv 4782969 \bmod 7 \equiv 2$ (because 4782969 leaves a remainder of 2, when divided by 7)

i.e., $45^{14} \equiv 2 \bmod 7$

Alternatively:

$$45^{14} \equiv 3^{14} \bmod 7 \equiv 3^{3\cdot 4+2} \bmod 7 \equiv 3^{3\cdot 4} \cdot 3^2 \bmod 7 \equiv \left(3^3\right)^4 \cdot 9 \bmod 7 \equiv \left(3^3\right)^4 \cdot 9 \bmod 7$$

$$\equiv \underbrace{(27)^4 \cdot 9 \bmod 7 \equiv (-1)^4 \cdot 9 \bmod 7}_{27 \equiv 6 \bmod 7 \equiv (-1) \bmod 7} \equiv 1 \cdot 9 \bmod 7 \equiv 2 \bmod 7$$

i.e., $45^{14} \equiv 2 \bmod 7$

(d) $36^{25} \equiv$ ____ $\bmod 5$

This number is probably too large to deal with directly. So we replace 36 with its equivalent value mod 5.

36 leaves a **remainder of 1** when divided by 5. Therefore, $36 \equiv 1 \bmod 5$

Consequently, $36^{25} \equiv 1^{25} \bmod 5 \equiv 1 \bmod 5$

i.e., $36^{25} \equiv 1 \bmod 5$

(e) $36^{15} \equiv$ ____ $\bmod 8$

This number is probably too large to deal with directly. So we replace 36 with its equivalent value mod 8.

36 leaves a **remainder of 4** when divided by 8.

Hence, $36^{15} \equiv 4^{15} \bmod 8 \equiv 1073741824 \bmod 8$

1073741824 leaves a remainder of 0 when divided by 8.

Therefore: $36^{15} \equiv 4^{15} \bmod 8 \equiv 1073741824 \bmod 8 \equiv 0$

i.e., $36^{15} \equiv 0 \bmod 8$

Alternatively:

$$36^{15} \equiv 4^{15} \bmod 8 \equiv 4^{2\cdot 7+1} \bmod 8 \equiv 4^{2\cdot 7} \cdot 4^1 \bmod 8 \equiv \left(4^2\right)^7 \cdot 4 \bmod 8 \equiv \underbrace{16^7 \cdot 4 \bmod 8 \equiv 0^7 \cdot 4 \bmod 8}_{16\equiv 0 \bmod 8}$$

$$\equiv 0 \bmod 8$$

i.e., $36^{15} \equiv 0 \bmod 8$

(f) $29^{11} \equiv \_\_\_\_ \bmod 5$

This number is probably too large to deal with directly. So we replace 29 with its equivalent value mod 5.

29 leaves a **remainder of 4** when divided by 5.

Hence, $29^{11} \equiv 4^{11} \bmod 5 \equiv 4194304 \bmod 5$

4194304 leaves a remainder of 4 when divided by 5.

Therefore: $29^{11} \equiv 4^{11} \bmod 5 \equiv 4194304 \bmod 5 \equiv 4 \bmod 5$

$$\boxed{\text{i.e., } 29^{11} \equiv 4 \bmod 5}$$

Alternatively:

$$29^{11} \equiv 4^{11} \bmod 5 \equiv 4^{2\cdot 5+1} \bmod 5 \equiv 4^{2\cdot 5} \cdot 4^1 \bmod 5 \equiv \left(4^2\right)^5 \cdot 4 \bmod 5 \equiv \left(4^2\right)^5 \cdot 4 \bmod 5$$

$$\equiv \underbrace{16^5 \cdot 4 \bmod 5 \equiv 1^5 \cdot 4 \bmod 5}_{16 \equiv 1 \bmod 5} \equiv 4 \bmod 5$$

$$\boxed{\text{i.e., } 29^{11} \equiv 4 \bmod 5}$$