**Name:** *Caleb McWhorter — Solutions*
**MATH 308**
**Fall 2022**
**HW 11: Due 11/04**

*"There are five elementary arithmetical operations: addition, subtraction, multiplication, division, and modular forms."*
*–Martin Eichler*

**Problem 1.** (10pt) Showing all your steps, compute the following:

(a) $(15+14) \mod 6$

(b) $(8-17) \mod 5$

(c) $-(1+8) \mod 3$

(d) $(20-11) \mod 8$

(e) $(9+7) \mod 4$

(f) $14(5) \mod 6$

(g) $2(3) \mod 7$

(h) $-7(4) \mod 9$

(i) $(-3)^3 \mod 4$

(j) $6^2 \mod 5$

**Solution.**

(a)
$$(15+14) \equiv (3+2) \equiv 5 \mod 6$$

(b)
$$(8-17) \equiv -9 \equiv 1 \mod 5$$

(c)
$$-(1+8) \equiv -9 \equiv 0 \mod 3$$

(d)
$$(20-11) \equiv 9 \equiv 1 \mod 8$$

(e)
$$(9+7) \equiv 16 \equiv 0 \mod 4$$

(f)
$$14(5) \equiv 2(5) \equiv 10 \equiv 4 \mod 6$$

(g)
$$2(3) \equiv 6 \mod 7$$

(h)
$$-7(4) \equiv 2(4) \equiv 8 \mod 9$$

(i)
$$(-3)^3 \equiv -27 \equiv 1 \mod 4$$

(j)
$$6^2 \equiv 1^2 \equiv 1 \mod 5$$

**Problem 2.** (10pt) Consider arithmetic modulo 4.

(a) List two positive elements and two negative elements of $[0]$ and $[3]$.

(b) Choose elements $x \in [1]$ and $y \in [3]$ with $x, y > 10$ and show that $[x]+[y] = [0]$; that is, use the division algorithm to write $x = 4m + r_x$ and $y = 4n + r_y$ and show $[x] + [y] = [r_x] + [r_y] = [0]$.

(c) Choose elements $x, y \in [2]$ with $x, y > 10$ and show that $[x] \cdot [y] = [0]$; that is, use the division algorithm to write $x = 4m + r_x$ and $y = 4n + r_y$ and show $[x] \cdot [y] = [r_x] \cdot [r_y] = [0]$.

**Solution.**

(a) We have $4, 8 \in [0]$ and $-4, -8 \in [0]$, and we have $3, 7 \in [3]$ and $-1, -5 \in [3]$. Generally, observe that $[0] = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$ and that the elements of $[0]$ are of the form $4k$ for some $k \in \mathbb{Z}$. Furthermore, observe that $[3] = \{\ldots, -9, -5, -1, 3, 7, 11, \ldots\}$ and that the elements of $[3]$ are of the form $4k + 3$ for some $k \in \mathbb{Z}$.

(b) Observe that $4(5) + 1 = 21 \in [1]$ and $4(4) + 3 = 19 \in [3]$. But then we have...

$$21 + 19 \equiv (4 \cdot 5 + 1) + (4 \cdot 4 + 3) \equiv 4(5 + 4) + (1 + 3) \equiv 0 + 4 \equiv 0 \mod 4$$

Generally, if $x \in [1]$, then $x = 4k + 1$ for some $k \in \mathbb{Z}$, and if $y \in [3]$, then $y = 4j + 3$ for some $j \in \mathbb{Z}$. But then...

$$x + y \equiv (4k + 1) + (4j + 3) \equiv 4(k + j) + (1 + 3) \equiv 0 + 4 \equiv 0$$

(c) Observe that $4(5) + 2 = 22 \in [2]$ and $4(8) + 2 = 34 \in [2]$. But then we have...

$$22 \cdot 34 \equiv (4 \cdot 5 + 2) \cdot (4 \cdot 8 + 2) \equiv 4(160) + 4(10) + 4(16) + 2 \cdot 2 \equiv 0 + 0 + 0 + 4 \equiv 0 \mod 4$$

Generally, if $x, y \in [2]$, then $x = 4k + 2$ and $y = 4j + 2$ for some $k, j \in \mathbb{Z}$. But then we have...

$$x \cdot y \equiv (4k + 2) \cdot (4j + 2) \equiv 4(4kj) + 4(2k) + 4(2j) + 2 \cdot 2 \equiv 0 + 0 + 0 + 4 \equiv 0 \mod 4$$

**Problem 3.** (10pt) Showing all your work, complete the following:

(a) Compute $\phi(7)$, $\phi(11)$, and $\phi(131)$.

(b) Compute $\phi(8)$, $\phi(9)$, and $\phi(49)$.

(c) Compute $\phi(360)$.

(d) How many integers $0, 1, 2, \ldots, 359$ are invertible modulo 360? Explain.

**Solution.**

(a) If $p$ is prime, we know that $\phi(p) = p - 1$. But then we have...

$$\begin{aligned} \phi(7) &= 7 - 1 = 6 \\ \phi(11) &= 11 - 1 = 10 \\ \phi(131) &= 131 - 1 = 130 \end{aligned}$$

(b) If $p$ is prime and $k \geq 1$, we know that $\phi(p^k) = p^{k-1}(p-1)$. But then we have...

$$\begin{aligned} \phi(8) &= \phi(2^3) = 2^2(2-1) = 4 \cdot 1 = 4 \\ \phi(9) &= \phi(3^2) = 3^1(3-1) = 3 \cdot 2 = 6 \\ \phi(49) &= \phi(7^2) = 7^1(7-1) = 7 \cdot 6 = 42 \end{aligned}$$

(c) We know that if $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a) \cdot \phi(b)$. But then using the fact that if $p$ is prime and $k \geq 0$, then $\phi(p^k) = p^{k-1}(p-1)$, and the fact that $360 = 2^3 \cdot 3^2 \cdot 5$, we have...

$$\phi(360) = \phi(2^3 \cdot 3^2 \cdot 5) = \phi(2^3) \cdot \phi(3^2) \cdot \phi(5) = 2^2(2-1) \cdot 3^1(3-1) \cdot (5-1) = 4 \cdot 6 \cdot 4 = 96$$

(d) If $a \in \{0, 1, \ldots, 359\}$, then $a$ is invertible mod 360, i.e. $a^{-1}$ exists, if and only if $\gcd(a, 360) = 1$. Therefore, we need to count the number of integers $0 \leq k \leq 359$ that are relatively prime to 360. However, $\phi(n)$ counts the number of integers $0 \leq k \leq n$ that are relatively prime to $n$. From (c), we know that $\phi(360) = 96$. Therefore, there are 96 integers between 0 and 359, inclusive, that are invertible modulo 360.

**Problem 4.** (10pt) Being sure to fully justify your responses, answer the following:

(a) Is 7 invertible modulo 15? Explain.

(b) Prove your claim in (a) by finding an inverse for 7 modulo 15 or showing that there is no inverse of 7 modulo 15.

(c) Is 2 invertible modulo 6? Explain.

(d) Prove your claim in (c) by finding an inverse for 2 modulo 6 or showing that there is no inverse of 2 modulo 6.

**Solution.**

(a) We know that $7^{-1}$ exists modulo 15 if and only if $\gcd(7, 15) = 1$. Because $\gcd(7, 15) = 1$, we know that 7 is invertible modulo 15.

(b) Observe that $7(13) \equiv 91 \equiv 1$ mod 15. Therefore, $7^{-1} \equiv 13$ mod 15.

(c) We know that $2^{-1}$ exists modulo 6 if and only if $\gcd(2, 6) = 1$. Because $\gcd(2, 6) = 2 \neq 1$, we know that 2 is not invertible modulo 6.

(d) We know that 2 is not invertible modulo 6 as...

$$\begin{aligned}
2 \cdot 0 &\equiv 0 \pmod 6 \\
2 \cdot 1 &\equiv 2 \pmod 6 \\
2 \cdot 2 &\equiv 4 \pmod 6 \\
2 \cdot 3 \equiv 6 &\equiv 0 \pmod 6 \\
2 \cdot 4 \equiv 8 &\equiv 2 \pmod 6 \\
2 \cdot 5 \equiv 10 &\equiv 4 \pmod 6
\end{aligned}$$