Math 546
Spring 2021
Justin Baum Homework 1

Problem 1a. Prove that if $a \equiv 1 \pmod{n}$ or $a \equiv -1 \pmod{n}$, then $a^2 \equiv 1 \pmod{n}$.

Solution: Given $a \equiv 1 \pmod{n}$, then there exists an integer k, $a = kn + 1$. Then $a^2 = k^2n + 2kn + 1 = (k^2 + 2k)n + 1$, thus $a^2 \equiv 1 \pmod{n}$.
Similarly $a \equiv -1 \pmod{n}$, then $a = kn - 1$. Thus $a^2 = k^2n - 2kn + 1 = (k^2 - 2k)n + 1$ and $a^2 \equiv 1 \pmod{n}$. □

Problem 1b. Give an example to show that the converse of the statement from part a. is not always true.

Solution: $2^2 \equiv 1 \pmod{3}$ but $2 \not\equiv 1 \pmod{3}$. □

Problem 2a. Prove that if $2x \equiv 2y \pmod{5}$, then $x \equiv y \pmod{5}$.

Solution: Assume $x \not\equiv y \pmod{5}$. Then $x = 5n + a$ and $y = 5m + b$, where $a, b, n, m \in \mathbb{Z}$, $a \neq b$, and $0 \leq a, b < 5$.

$$2x = (2)5n + 2a \text{ and } 2y = (2)5m + 2b$$

We saw in class that $2[x]_5 \neq 2[y]_5$ because $\gcd(2, 5) = 1$. Thus $2x \not\equiv 2y \pmod{5}$.

□

Problem 2b. Give an example of integers x, y such that $2x \equiv 2y \pmod{26}$, but $x \not\equiv y$ (mod 2)6.

Solution: $x = 13$, $y = 0$, $2(13) \equiv 2(0) \pmod{26}$, but $13 \not\equiv 0 \pmod{26}$. □

Problem 3. Which of the following classes have a multiplicative inverse? If the multiplicative inverse exists, find it. If it does not exist, explain why it does not exist.

1. $[2]_5$ *Solution:* $2^{-1} \equiv 3 \pmod{5}$.

$$3(5k + 2) \equiv (3)5k + 6 \equiv (3)5k + 5 + 1 \equiv 5(3k + 1) + 1 \pmod{5}$$

□

2. $[4]_6$ *Solution:* Assume there was a multiplicative inverse, x. $4x \equiv 1 \pmod{6}$. However $4x \pmod{6}$ is always even, thus there does not exist a multiplicative inverse.
We can also check by exhaustion.

- $0(4) = 0 \pmod{6}$
- $1(4) = 4 \pmod{6}$
- $2(4) = 2 \pmod{6}$
- $3(4) = 0 \pmod{6}$
- $4(4) = 4 \pmod{6}$
- $5(4) = 2 \pmod{6}$

□

3. $[7]_{11}$ *Solution:* $7^{-1} \equiv 8 \pmod{11}$.

$$8(11k + 7) \equiv 8(11k) + 56 \equiv 11(8k + 5) + 1 \pmod{11}$$

□