Unit 3: A Modular World

Paul Ycay
MATH 409

December 13, 2019

The following theorems are ones to be marked. There is a separate file of handwritten notes for the rest of the theorems in this chapter

Exercise 3.5. Find the remainder of $39|17^{48} - 5^{24}$

Solution. We can take the *modulo of* 13 instead of 39 as $13|39$ and $13 < 17$. Thus, we know that

$$\begin{aligned} 17 &\equiv 4 \ (mod\ 13) \\ 17^2 &\equiv 4^2 \ (mod\ 13) \\ 17^2 &\equiv 3 \ (mod\ 13) \\ (17^2)^3 &\equiv 3^3 \ (mod\ 13) \\ 17^6 &\equiv 1 \ (mod\ 13) \\ (17^6)^8 &\equiv 1^8 \ (mod\ 13) \\ 17^{48} &\equiv 1 \ (mod\ 13) \end{aligned}$$

Similarly,

$$\begin{aligned} 5 &\equiv 5 \ (mod\ 13) \\ 5^2 &\equiv -1 \ (mod\ 13) \\ (5^2)^{12} &\equiv (-1)^{12} \ (mod\ 13) \\ 5^{24} &\equiv 1 \ (mod\ 13) \end{aligned}$$

Thus,

$$\begin{aligned} &[17^{48} - 5^{24}]_{39} \\ &= [17^{48}]_{39} - [5^{24}]_{39} \\ &= 1 - 1 = 0 \end{aligned}$$

Thus, the remainder is 0. □

Theorem 3.7. Let $f(x) = 13x^{49} - 27x^{27} + x^{14} - 6$. Is it true that $f(98) \equiv f(-100)\ (mod 99)$?

Proof. We know that $98 \equiv -1\ (mod\ 99)$. Thus, $f(98) \equiv f(-1)\ (mod\ 99)$ implies

$$\begin{aligned} &[13(-1)^{49} - 27(-1)^{27} + (-1)^{14} - 6]_{99} \\ &[-13 + 27 + 1 - 6]_{99} \\ &9 \end{aligned}$$

Furthermore, $-100 \equiv -1\ (mod\ 99)$ implies that $f(-100) \equiv f(-1)\ (mod\ 99)$. Then

$$\begin{aligned} &[13(-1)^{49} - 27(-1)^{27} + (-1)^{14} - 6]_{99} \\ &[-13 + 27 + 1 - 6]_{99} \\ &9 \end{aligned}$$

Thus, proved. □

Theorem 3.14. Given any integer a and any natural number n, there exists a unique integer t in the set $0, 1, 2, \dots, n-1$ such that $a \equiv t\ (mod\ n)$

Proof. Suppose $a \in Z$. By Division Algorithm, there exists $t, q \in Z$ such that $a = nq + t$, where $0 \leq t < n$. Then $a - t = nq \implies n|a - t$. By definition of congruence, $a \equiv t\ (mod\ n)$. In other words, a has to be congruent to at least one of the elements in the set $0, 1, 2, \dots, n-1$ since we claimed $0 \leq t < n$. □

Theorem 3.16. Let n be a natural number. Every complete residue system *modulo* n contains n elements.

Proof. Denote the set $A := 0, 1, 2, \dots, n-1$ to be a complete residue system $mod\ n$. Suppose $|A|$ (the size of A) is greater than n. By the Pigeonhole Principle, at least two elements in A will have the same remainder when divided by n. This contradicts the fact that A is a complete residue system $mod\ n$. Thus, $|A| \leq n$. □

Theorem 3.19. Let $a,\ b,\ and\ n$ be integers with $n > 0$. Show that $ax \equiv b\ (mod\ n)$ has a solution if and only if there exists integers x and y such that $ax + ny = b$.

Proof. Proof of the 1st part. Suppose $ax \equiv b\ (mod\ n)$, with $a, b, n \in Z$ and $n > 0$. Then $ax - b = nt$, for some $t \in Z$. Since t is an integer, let $t = -y$. Thus, $ax - b = n(-y) \implies ax + ny = b$.
Proof of the 2nd part. Given $ax + ny = b$, for integers $x, y, n, n > 0$. Then $ax + ny = b \implies ax - b = -ny \implies ax - b = n(-y) \implies n|ax - b \implies ax \equiv b\ (mod\ n)$. Thus, proved. □

Theorem 3.20. Let $a, b, n \in Z$ with $n > 0$. The equation $ax \equiv b\ (mod\ n)$ has a solution if and only if $(a, n)|b$.

Proof. Proof of the 1st part. Given $ax \equiv b \ (mod\ n)$, $a, b, n \in Z$ with $n > 0$, then $n|ax - b \implies ny = ax - b \implies b = ax - ny,\ y \in Z$. Fix $t = (a, n)$. Then, $t = ac + nd,\ c, d \in Z$. Thus, $t|a$ and $t|n$. So, for integers $f_1, f_2 \in Z$, we have $a = tf_1\ and\ n = tf_2$. From the equation $b = ax - ny$, apply substitution

$$\begin{aligned} b &= (tf_1)x - (tf_2)y \\ b &= t(f_1x - f_2y) \\ b &= tg,\ g \in Z \end{aligned}$$

Then $t|b \implies (a, n)|b$.
Proof of the 2nd part. Fix $t = (a, n)$. Then $t = ac + nd,\ c, r \in Z$. Since $t|b, b = tg = (ac + nr)g,\ g \in Z$. Then, $b = acg + nrg$

$$\begin{aligned} nrg &= b - a(cg) \\ n(y) &= b - a(x) && x, y \in Z \\ -n(y) &= ax - b \\ n(-y) &= ax - b && \because y \in Z \end{aligned}$$

Thus, $ax \equiv b \ (mod\ n)$. $\square$